Draft National Infrastructure Protection Plan

Base Plan

November 2, 2005

This document is a For-Comment-Only draft that is being provided solely to effect the extensive coordination with Federal departments and agencies; State, Territorial, tribal, and local government entities; regional initiatives; and the private sector that is required for the development of the National Infrastructure Protection Plan.

Preface

Note: This section will contain the preface.

Letter of Agreement

The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of CI/KR protection efforts into a single national program. The NIPP identifies how homeland security partners will develop and implement a national effort to protect CI/KR across all sectors. The NIPP provides an overall framework integrating programs and activities that are currently underway in the various sectors, as well as new and developing CI/KR protection efforts. This collaborative effort between the private sector; State, Territorial, tribal, and local governments; regional initiatives; nongovernmental organizations; and the Federal Government will result in the prioritization of protection initiatives and investments across sectors to ensure that resources are applied where they offer the most benefit for reducing risk, deterring threats, and minimizing the consequences of attacks.

By signing this letter of agreement, HSPD-7 designated Sector-Specific Agencies and other Federal departments and agencies with special functions related to CI/KR protection commit to:

- Supporting NIPP concepts, framework, and processes and carrying out their assigned functional responsibilities regarding the protection of CI/KR, as described herein;
- Working with the Secretary of Homeland Security as appropriate and consistent with their own agency-specific authorities, resources, and programs to coordinate funding and implementation of programs that enhance CI/KR protection;
- Cooperating and coordinating with the Secretary of Homeland Security, in accordance with guidance provided in HSPD-7, as appropriate and consistent with their own agency-specific authorities, resources, and programs to facilitate CI/KR protection;
- Developing or modifying existing interagency and agency-specific CI/KR plans to facilitate compliance with the NIPP;
- Developing and maintaining partnerships with appropriate State, Territorial, local, tribal, regional, and international entities, the private sector, and nongovernmental organizations; and
- Protecting critical infrastructure data according to the Protected Critical Infrastructure Information (PCII) Program or appropriate guidelines, and sharing NIPP-related information as appropriate and consistent with their own agency-specific authorities.

Signatory departments and agencies follow.

Signatories

Note: This section will contain the listing of the signatories to the Letter of Agreement

Letter of Instruction

Note: This section will contain implementation guidance

Table of Contents

List of Tables and Figures

Figures

Tables

1 Introduction

Protecting the Critical Infrastructures and Key Resources (CI/KR) of the United States is essential to the Nation's security, economic vitality, and way of life. Attacks on CI/KR could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident. Direct attacks could result in large-scale human casualties and property destruction, and also profoundly damage national prestige, morale, and confidence. Attacks using components of the Nation's CI/KR as "weapons of mass destruction" could have even more devastating physical and psychological consequences.

In today's highly technical and digital world, attacks may manifest themselves in many forms, including both physical and cyber threats. In addition, the potential impacts of any one incident may affect a variety of other assets and systems. The interconnected and interdependent nature of the Nation's CI/KR makes it difficult—not to mention irresponsible—to attempt to address the protection of physical and cyber assets in isolation.

Protection of the Nation's CI/KR is one of six critical mission areas assigned to the Department of Homeland Security (DHS) by the Homeland Security Act of 2002. Additionally, the *National Strategy for Homeland Security* established the national CI/KR vision to:

> *…forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets [resources[1]] from terrorist attacks. Our country will continue to take immediate and decisive actions to protect assets and systems that could be attacked with catastrophic consequences…*

The National Strategy further established the need for a National Infrastructure Protection Plan (NIPP) as the primary vehicle to:

> *…organize the complementary efforts of government and private institutions to raise security over the long term to levels appropriate to each target's vulnerability and criticality. The Federal Government will work to create an environment in which State, local, and private entities can best protect the infrastructures they control.*

Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection, issued by the President on December 17, 2003, provided the clear direction to implement this vision, and mandated development of the NIPP as the primary vehicle to guide protection of the Nation's CI/KR. HSPD-7 designated the Secretary of the DHS as the "principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources."

In this capacity, DHS is responsible for coordinating and implementing the development of the NIPP with participation from a wide range of government and private sector security partners. This responsibility includes addressing the complexities of the Nation's Federal system of government, its multifaceted and interdependent economy, and the need for close cooperation between the private sector and government at all levels to initiate and sustain effective protective measures.

[1] The *National Strategy for Homeland Security* uses the term "key assets," defined as individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. The Homeland Security Act of 2002 and HSPD-7 uses the term "key resources," defined more generally to capture publicly or privately controlled resources essential to the minimal operations of the economy or government. "Key resources" is the current terminology.

The NIPP provides a consistent, unifying structure for the integration of both existing and future CI/KR protection efforts. It outlines the core processes and mechanisms DHS and its security partners will use to implement key protection initiatives. In addition, NIPP Sector-Specific Plans (SSPs) will detail the application of the NIPP core processes specific to each CI/KR sector. The SSPs are developed by HSPD-7-designated Federal Sector-Specific Agencies (SSAs) in coordination with other security partners in accordance with guidance provided by DHS.

The ongoing planning and coordination processes for the NIPP and the SSPs are structured to ensure that public and private resources are focused where their costs and benefits will produce the greatest reduction in risk within, and across, the CI/KR sectors. Success will require working together through public- and private-sector partnerships to identify, analyze, prioritize, and enhance the protection of the Nation's CI/KR.

1.1 All-Hazards and CI/KR Protection

The Nation's CI/KR generally are robust and resilient. This is the result of decades of experience responding to natural disasters, industrial accidents, and the deliberate acts of malicious individuals. Private sector infrastructure owners and operators and government emergency managers and first responders have developed expertise in preparing for and responding to a wide variety of natural and manmade hazards. In contrast, preparing for and responding to terrorist threats against CI/KR present relatively new and highly complex challenges; as a consequence, the Presidential guidance and strategies outlined above focus a national effort on this emerging threat.

Using the NIPP framework to enable protection of America's CI/KR not only makes the nation more secure from terrorist attacks, but also helps to reduce vulnerability to natural disasters, manmade accidents, organized crime, and computer hackers. As a result, the NIPP provides a foundation for a broader set of protection and preparedness imperatives that address all hazards. The NIPP overarching mechanisms that pay these additional benefits in an all-hazards environment include:

- A unified and comprehensive approach that integrates authorities, capabilities, and resources on a national scale;
- A complete and accurate assessment of America's CI/KR that not only enables prioritization of protection efforts, but also aids greatly during response and recovery efforts;
- An organization and coordinating structure to enable effective partnership with State, Territorial, tribal and local governments as well as the private sector;
- An integrated approach to securing the cyber and physical aspects of the Nation's CI/KR in which cyber and physical measures complement one another; and
- The development and use of sophisticated analytical and modeling tools to develop effective protective solutions.

1.2 The Terrorist Threat to the Nation's CI/KR

1.2.1 Characteristics of Terrorism

The number of high-profile terrorist attacks that have occurred following the September 11, 2001 attacks on the Pentagon and the World Trade Center underscores the determination and resiliency of Islamic extremist terrorist organizations that have declared war against the West. Such terrorists—namely those within the broader Sunni extremist movement, to include al-Qaida and its affiliated elements—have proven to be relentless and patient, in addition to being opportunistic and flexible. They have learned from experience and modified their tactics and targets to exploit perceived vulnerabilities and avoid observed strengths. As security increases around more predictable targets, in the future they may shift their focus to less protected ones. Enhancing countermeasures for any one terrorist tactic or target,

therefore, makes it more likely that terrorists will favor another. Although our information about possible terrorist targets is incomplete, everything we do know about terrorist goals and motivations point to possible strikes against America's vast array of CI/KR.

1.2.2 The Nature of Possible Attacks

Terrorist organizations such as al-Qaida and its affiliates have shown an understanding of the potential consequences of carefully planned attacks on economic, transportation, and symbolic targets both within the United States and abroad. Future terrorist attacks against CI/KR across the United States could seriously threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence. Additionally, terrorist attacks against these targets may represent an attempt by the attacker to promote the terrorist agenda or erode the public confidence in the U.S. Government or its policies.

Although a degree of uncertainty remains as to how, why, and when a particular target might be attacked by extremist terrorists, DHS has considered a broad range of terrorist objectives, intentions, and capabilities and believes that attacks against the U.S. CI/KR are contemplated to achieve three general types of effects:

- **Direct infrastructure effects:** Cascading disruption or arrest of the functions of CI/KR through direct attacks on a critical node, system, or function.
- **Indirect infrastructure effects:** Cascading disruption and financial consequences for government, society, and economy through public- and private sector reactions to an attack. An operation could reflect an appreciation of interdependencies between different elements of the infrastructure, as well as the psychological importance in demonstrating the ability to strike effectively in the United States.
- **Exploitation of infrastructure:** Exploitation of elements of a particular infrastructure to disrupt or destroy another target. Attacks using infrastructure as a weapon to strike other targets allows for the magnification of capabilities far beyond what the terrorist organization could do using its organic capabilities.

The NIPP outlines the ways in which DHS and its security partners use threat analysis to inform comprehensive risk assessments. The approach outlined in Chapter 3 strikes a balance between the specific and the general, ensures that plausible attack scenarios are broad enough to avoid a "failure of imagination," and contains sufficient detail to enable quantitative and qualitative risk assessment.

1.2.3 The Vulnerability of the U.S. Infrastructure to Attack

America is an open and technologically complex nation with a wide array of CI/KR that spans important aspects of government, economy and society. The majority of these infrastructures and resources are owned and operated by the private sector, and State, Territorial, tribal, or local governments. The Nation's CI/KR is comprised of a vast number of highly-interconnected facilities, systems, and functions. This pervasive dynamic further characterizes them as highly lucrative potential targets for terrorist exploitation.

Because of this, protecting U.S. CI/KR is an enormous challenge. While it is not possible to protect or eliminate the vulnerability of all CI/KR throughout the country, strategic improvements in security can make it more difficult to mount successful attacks and serve to lessen their impact.

1.3 Purpose of the NIPP

The NIPP provides an integrated, comprehensive approach to addressing physical, cyber, and human threats and vulnerabilities. It uses a risk-based approach to enhance security and mitigate the risk of terrorist attack to the Nation. The Plan's risk management framework prioritizes CI/KR protection activities both within and across sectors based on threats, vulnerabilities, and consequences.

The NIPP defines the processes and mechanisms that allow security partners to prioritize protection investments and initiatives so that resources are applied where they offer the most benefit for reducing vulnerability, deterring threats, and minimizing the consequences of attacks. Implementing the NIPP will involve the integrated, coordinated support of security partners with infrastructure protection responsibilities across the country.

The NIPP provides the framework and sets the direction for implementing this coordinated, national effort. It provides a mechanism for identifying CI/KR, understanding threats, assessing vulnerabilities, prioritizing investments based on costs and benefits, and implementing protection measures within and across each CI/KR sector. The NIPP delineates roles and responsibilities for security partners in carrying out these activities, while respecting the authorities, jurisdictions, and prerogatives of these partners.

1.4 Scope and Applicability

This section describes the overall scope and applicability of the NIPP.

1.4.1 Scope

In accordance with the policy directives established in HSPD-7, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, and the *National Strategy to Secure Cyberspace*, the NIPP focuses specifically on the challenges of protecting the Nation's CI/KR from acts of terrorism. It builds on, and is structured to be consistent with, the Nation's all-hazards approach to homeland security preparedness and domestic incident management, focusing on the protection of CI/KR from the unique and potentially catastrophic impacts of terrorist attacks.

The NIPP addresses ongoing and future activities within the 17 CI/KR sectors identified in HSPD-7, and across the sectors nationally. It defines processes and mechanisms used to prioritize protection of CI/KR within U.S. borders, and to address the interconnected CI/KR global infrastructures and networks upon which the Nation depends. The processes outlined in the NIPP and the SSPs recognize that protective measures do not stop at a facility's fence line or a national border; but also consider the requirements of trans-border infrastructures, international vulnerabilities, and global and sector dependencies and interdependencies.

1.4.2 Applicability

The NIPP covers the full range of CI/KR sectors as defined in HSPD-7. The framework is applicable to all security partners with CI/KR protection responsibilities and includes explicit roles and responsibilities for the Federal Government, including CI/KR under the control of the legislative, executive, or judicial branches. The NIPP also provides an organized structure, protection guidelines, and recommended activities for other security partners to help ensure consistent implementation of the framework and the most effective use of resources. Finally, the NIPP provides mechanisms to enhance CI/KR protection efforts in an all-hazards environment.

1.5 Goal and Objectives

The overarching goal of the NIPP is to:

> *Enhance protection of the Nation's CI/KR in order to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to "destroy, incapacitate, or exploit" them.*

Achieving this goal focuses on three principal objectives:

- Building security partnerships to implement CI/KR protection programs;
- Implementing a long-term risk-reduction program; and
- Maximizing efficient use of resources for CI/KR protection.

1.5.1 Building Security Partnerships

Building security partnerships is the foundation of the national CI/KR protection effort. These partnerships and coordinating structures provide a framework to:

- Establish effective coordinating structures and information-sharing processes and protocols among security partners;
- Enhance coordination with the international community; and
- Build public awareness.

Chapters 2 and 4 detail the roles and responsibilities and the mechanisms for the leadership, coordination, and information-sharing necessary to enable effective partnerships.

1.5.2 Implementing a Long-Term CI/KR Risk-Reduction Program

The long-term risk-reduction program detailed in the NIPP includes processes to:

- Establish a risk management framework to guide CI/KR protection programs;
- Identify and regularly update the status of CI/KR protection programs within and across sectors;
- Conduct and update risk assessments at the asset, sector, cross-sector and transnational levels;
- Analyze, store, and share risk assessment data consistent with relevant legal requirements;
- Develop and deploy new technologies to protect CI/KR;
- Provide a system for continuous measurement and improvement of CI/KR protection activities, including:
  - Establishing performance metrics to assess the effectiveness of protective measures; and
  - Updating the NIPP and SSPs, as required.

The NIPP also specifies the processes, key initiatives, and milestones necessary to implement an effective long-term CI/KR risk-reduction program. Chapters 3 and 6 provide details regarding the risk management framework, program structure; elements, and funding mechanisms; planning initiatives; and performance measures, respectively.

1.5.3 Maximizing Efficient Use of Resources for CI/KR Protection

Maximizing efficient use of resources for CI/KR protection includes a coordinated and integrated annual process for program implementation that:

- Prioritizes assets within and across sectors;
- Informs the annual Federal process regarding planning, programming and budgeting for national-level protection activities;
- Aligns the resources of the Federal budget to the CI/KR protection mission;
- Takes into account State and local government decisions relating to planning, programming, and budgeting;
- Identifies potential incentives for security-related activities where they do not naturally exist in the marketplace;
- Draws on expertise across organizational and national boundaries; and
- Shares lessons learned to leverage expertise and reduce redundant efforts.

Chapter 7 describes the processes required to set the annual CI/KR protection agenda to include appropriate coordination with SSAs and other security partners regarding resource allocation. Also discussed are processes to utilize grant programs, regulatory, and other funding authorities to maximize use of resources to support program priorities.

Efficient use of resources requires a deliberate process to continuously improve technology, databases and data systems used to protect CI/KR and manage risk. These processes are detailed in Chapter 6.

1.6 Planning Assumptions

The NIPP is based on the planning assumptions and special considerations included in this section.

1.6.1 Sector-Specific Nature of CI/KR Protection

- Approaches to CI/KR protection and risk management vary based on sector characteristics, requirements, and maturity;
- Assets and systems vary in criticality from one sector or jurisdiction to another;
- Many assets and systems are dependent on multiple elements and networks to function, both at the sector and local levels. In some cases, a failure in one sector will significantly impact another sector's ability to perform necessary functions;
- Successful CI/KR protection requires more robust baseline data on assets within and across CI/KR sectors, regions, and specific localities;
- Private sector firms conduct risk management planning and invest in security from a business perspective; and
- Strong relationships between security partners are essential to meet the CI/KR protection goals set forth in the NIPP.

1.6.2 Adaptive Nature of the Terrorist Threat

- CI/KR protection activities take place in a highly dynamic threat environment. The general threat environment changes as the capabilities and the intentions of terrorists evolve;
- It is not possible to protect all assets against every possible terrorist attack without bringing the national economy and way of life to a virtual standstill. A risk-based approach driven by intelligence analysis and reporting is crucial to an effective risk mitigation strategy and efficient resource allocation;
- Given the uncertain nature of the threat, prudent planning requires that all plausible threats, not just the most likely threat scenarios, be regarded when considering ways to enhance the protection of CI/KR; and
- Prevention of terrorist acts requires a proactive approach to enhance decision making processes, provide advance warning to potentially targeted CI/KR, and assist CI/KR owners and operators in taking protective steps to preempt terrorist plots.

1.6.3 Applicability to an All-Hazards Environment

- Natural disasters such as floods, hurricanes, tornadoes, wildfires, and earthquakes, and unintentional manmade hazards, such as oil spills or nuclear power plant accidents, also pose complex threats to the Nation's CI/KR; and
- Efforts to enhance the protection of CI/KR from terrorist attacks also benefit CI/KR all-hazards preparedness and response in many situations.

1.7 Special Considerations

Special considerations exist for the cyber dimension, components of the human element, and the complex international relationships required for CI/KR protection.

1.7.1 The Cyber Dimension

- The NIPP cyber dimension spans cyber infrastructure (including, but not limited to, the Internet) and associated cybersecurity systems;
- Cyber infrastructure includes electronic information and communications systems and the information contained in those systems. Information and communication systems are comprised of all the hardware and software that processes (i.e., creates, accesses, modifies, and destroys), stores (e.g., all media types: paper, magnetic, and electronic), and communicates (i.e., shares and distributes) information, or any combination of all of these elements. For example, computer systems and networks, such as the Internet, are part of cyber infrastructure;
- "Producers" of cyber infrastructure are the Information Technology (IT) industrial base, which comprise the IT Sector;
- "Consumers" of cyber infrastructure must maintain security in a changing threat environment. Individuals, whether private citizens or employees with cyber systems administration responsibility, play a significant role in managing the security of computer systems to ensure that they are not used to enable attacks against CI/KR;
- Cybersecurity includes the prevention of damage to, unauthorized use or exploitation of, and, if needed, the restoration of electronic information and communications systems (and the information contained therein); to ensure confidentiality, integrity, and availability; and
- Functions and services within and across sectors are enabled through cyber infrastructure. If cybersecurity is not integrated appropriately, the risk to sector operations is greatly increased.

1.7.2 Components of the Human Element

- The NIPP recognizes that each CI/KR asset is made of component physical, cyber, and human elements;
- The human element requires consideration of the following:
    - Identifying and preventing the "insider threat" resulting from infiltration or individual employees determined to do harm;
    - Identifying and protecting critical functions, information, and employees from terrorist attack;
- Assessing human element vulnerabilities is more subjective than assessing the physical vulnerabilities of corresponding systems and structures; and
- Diverse protective programs and actions to address threats posed by employees and to employees need to be put into place across the country.

1.7.3 International CI/KR Protection

- The NIPP addresses international CI/KR protection, including interdependencies and asset vulnerabilities based on threats that originate outside the country;
- The United States works with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber infrastructures and products. Specific initiatives

include ensuring Internet resiliency and quality assurance of foreign-produced software, and establishing a survivable network for CI/KR protection, communication and cooperation, alert, and notification;

- Protection of physical assets located on or near the borders with Canada and Mexico may require coordination with, and planning and/or sharing resources among neighboring countries;
- The U.S. Government and corporate America have a significant number of facilities located overseas that may be considered CI/KR; and
- Special consideration is required when infrastructure is extensively integrated into an international or global market (e.g., financial services, energy, or transportation) or when the proper functioning of a sector relies on inputs that are not within control of U.S. entities. For example, tampering with or disrupting the flow of critical raw materials into the United States(e.g., by contaminating agricultural products, obstructing transport of energy resources or industrial raw materials, or intentionally designing fatal flaws in software) may cause cascading failures within or across regions or sectors.

1.8 Authorities

Various statutes and policies provide the basis for Federal actions to implement the NIPP and associated CI/KR protection programs. The *Homeland Security Act of 2002*, the *National Strategy for Homeland Security*, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *National Strategy to Secure Cyberspace*, HSPD-7, and other relevant agency-specific statutory authorities provide the foundation for the NIPP.

This section outlines the guiding statutes and policies and addresses the relationship between the NIPP and other elements of the Nation's homeland security framework, including HSPD-5, Management of Domestic Incidents, and HSPD-8, National Preparedness. Appendix B, Summary of Relevant Authorities, provides a list of statutes and HSPDs relating to NIPP processes and procedures.

Figure 1-1 depicts the relationship between the strategies, Presidential guidance documents, national initiatives, and plans that represent an overarching national framework for preparedness. Beginning with the Homeland Security Act of 2002, this system of strategies, directives, and plans provides a common nationwide approach to preparedness through interlocking prevention, protection, response, and recovery activities. The components of this system are discussed below.

1.8.1 The National Strategy for Homeland Security

The President's *National Strategy for Homeland Security* established protection of America's CI/KR as a core homeland security mission and a key element of the comprehensive approach to homeland security and domestic incident management. The Homeland Security Strategy articulated the vision for a unified "American Infrastructure Protection effort" to "ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency" and to "assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to the country, instead of inadvertently shifting risk from one potential set of targets to another."

The strategy called for the development of "interconnected and complementary homeland security systems that are reinforcing rather than duplicative and that ensure essential requirements are met," and "provide a framework to align the resources of the Federal budget directly to the task of securing the homeland."

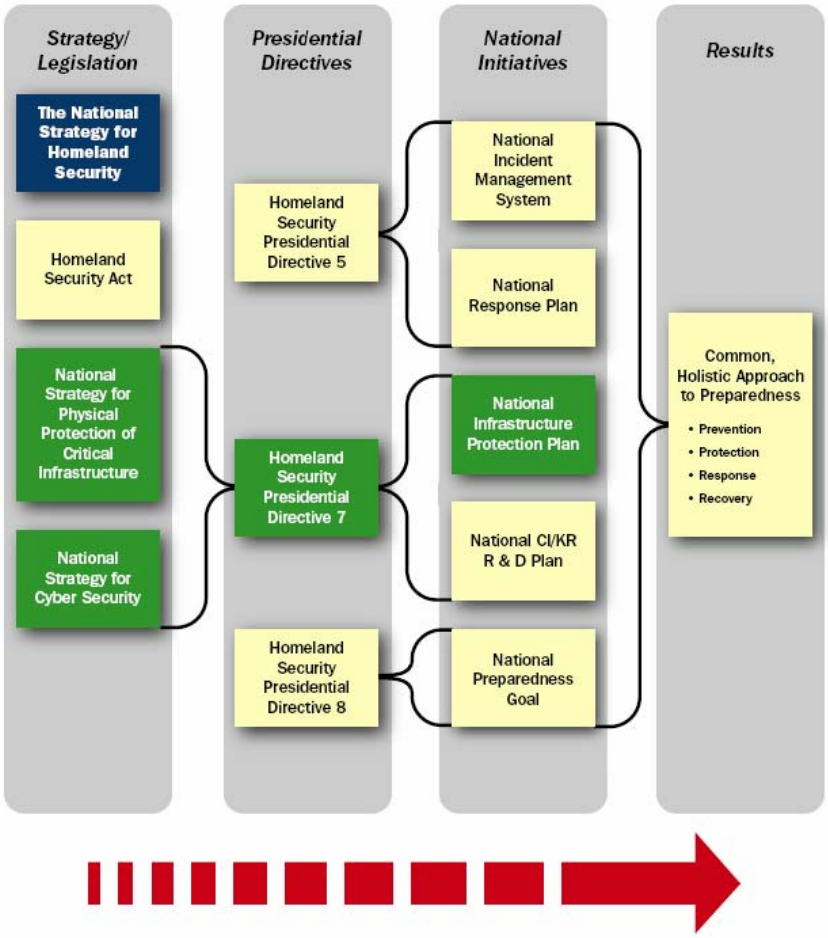


Figure 1-1. Homeland Security Authorities

1.8.2 The Homeland Security Act of 2002

The Homeland Security Act of 2002 established the DHS mission to include: "reducing the Nation's vulnerability to terrorist attacks" and charged the new department with the responsibility for evaluating vulnerabilities and ensuring that steps are implemented to protect high-risk elements of America's CI/KR, including food and water systems, agriculture, health systems and emergency services, information technology and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and National monuments and icons. Title II, Section 201 of the Act assigned primary responsibility to DHS for developing a comprehensive national plan for securing CI/KR and for "taking or seeking to effect necessary measures to protect those key resources and infrastructures."

1.8.3 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets identified national policy, goals, objectives, and principles for actions needed to "secure the infrastructures and assets vital to national security, governance, public health and safety, economy and public confidence." The strategy also provides a unifying organization and identifies specific initiatives to drive near-term national protection priorities and inform the resource allocation process. Further, it establishes a foundation for building and fostering the cooperative environment in which government, industry, and private citizens can carry out their respective protection responsibilities more effectively and efficiently.

This Strategy includes the challenges and key initiatives needed to secure each of the CI/KR sectors and addresses specific "Cross-Sector Security Priorities" in five areas:

I. Planning and Resource Allocation;

II. Information sharing and indications and warnings;

III. Personal Surety, Building Human Capital, and Awareness;

IV. Technology and Research and Development (R&D); and

V. Modeling Simulation and Analysis.

1.8.4 The National Strategy to Secure Cyberspace

The National Strategy to Secure Cyberspace set forth strategic objectives and specific actions to prevent cyber attacks against America's CI/KR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from cyber attacks. The National Strategy to Secure Cyberspace articulates five national priorities, including:

I. A National Cyberspace Security Response System;

II. A National Cyberspace Security Threat and Vulnerability Reduction Program;

III. A National Cyberspace Security Awareness and Training Program;

IV. Securing Governments' Cyberspace; and

V. National Security and International Cyberspace Security Cooperation.

The first priority focuses on improving the national response to cyber incidents. The second, third, and fourth priorities are focused on reducing threats from, and vulnerabilities to, cyber attacks. The fifth priority involves preventing cyber attacks that could affect national security assets and to improve the international management of and response to such attacks.

1.8.5 Homeland Security Presidential Directives

Homeland Security Presidential Directives establish national policies and executive mandates for specific programs and activities. HSPD-1, establishing the Homeland Security Council, was issued on October 29, 2001, shortly after the September 11 attacks. It was followed by a series of directives regarding homeland security missions and functions. This section addresses the HSPDs that are most relevant to the CI/KR protection and related preparedness and incident management missions.

1.8.5.1 Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection

HSPD-7, issued by the President on December 17, 2003, established U.S. policy for "enhancing protection of the Nation's CI/KR." It mandated development of the NIPP as the primary vehicle for implementing the CI/KR protection policy. HSPD-7 directed the Secretary of Homeland Security to lead development of the plan, to include, but not limited to, the following four key elements:

- A strategy to identify, prioritize, and coordinate the protection of CI/KR;
- A summary of activities to be undertaken to define and prioritize, reduce the vulnerability of, and coordinate protection of CI/KR;
- A summary of initiatives for sharing information and for providing threat and warning data to State, Territorial, tribal, and local governments and the private sector; and

- Coordination and integration, as appropriate, with other Federal emergency management and preparedness activities, including the National Response Plan and guidance provided in the National Preparedness Goal.

1.8.5.2 Homeland Security Presidential Directive 5.Management of Domestic Incidents

HSPD-5, issued February 2003, required DHS to lead a coordinated national effort with other Federal departments and agencies, State, Territorial, tribal, and local governments, and the private sector, to develop and implement a National Incident Management System (NIMS) and the National Response Plan (NRP):

- The **NIMS**, issued March 1, 2004, provides a nationwide template enabling Federal, State, Territorial, tribal, and local governments, and private sector, and nongovernmental organizations to work together effectively and efficiently to prevent, prepare for, respond to, and recover from, incidents **regardless of cause, size, and complexity.**

- **The NRP**, built on the NIMS template and signed by 29 Federal departments and agencies and three nongovernmental organizations, was issued on December 15, 2004, and fully implemented on April 14, 2005. It establishes a single, comprehensive framework for the management of high-impact events, termed Incidents of National Significance, that require DHS coordination and effective response by an appropriate combination of Federal, State, Territorial, tribal, and local governments, and private sector, and nongovernmental organizations.

1.8.5.3 Homeland Security Presidential Directive 8, National Preparedness

HSPD-8, issued December, 2003, mandated development of a National Preparedness Goal aimed at helping entities at all levels of government build and maintain the capabilities to prevent, protection against, respond to, and recover from, major events or Incidents of National Significance, as defined in the NRP and NIMS. The preparedness goal is structured to help entities develop and maintain the capabilities needed to identify, prioritize, and protect infrastructure against terrorist attacks.

> National Preparedness Goal
>
> ***"To engage Federal, State, Territorial, tribal, and local entities, their private and nongovernmental partners, and the public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property and the economy."***

The National Preparedness Goal provides readiness targets, priorities, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness. To focus efforts and resources, it specifies seven national priorities (three that are overarching and four that are geared to building specific capabilities) designed to address the most urgent preparedness needs. Building capabilities to help enhance the Nation's CI/KR protection efforts are key elements in four of the seven priorities. Implementation of the NIPP is one of the Preparedness Goal's overarching priorities. The other two overarching priorities are implementation of NIMS and NRP. The capability-specific priorities that relate directly to the NIPP include strengthening: information sharing and collaborative capabilities; interoperable communications capabilities; and chemical, biological, radiological, nuclear, or explosive detection, response, and decontamination.

The NIPP and NRP are complementary plans that span a spectrum of homeland security mission areas: prevention, protection, response, and recovery. The NIPP establishes the Nation's "steady-state" level of protection by focusing resources where investment yields the largest reduction in national risk relative to cost. The NRP addresses prevention, preparedness, response, and recovery in the context of domestic

threat and incident management and Incidents of National Significance. Development of increased protective measures corresponding to the threat levels established in the Homeland Security Advisory System (HSAS) provides the bridge between "steady-state" operations using the NIPP framework and incident management activities using the NRP. When an Incident of National Significance occurs, regardless of cause, the NIPP framework provides the CI/KR protection dimension in support of the NRP coordinating structures. Further discussion of the relationship of the NIPP to the NRP, NIMS and the National Preparedness Goal is included in Chapter 5.

2 Responsibilities

> **"The kind of true partnership that protecting the homeland requires means that we not only share information but also responsibility. It means that we not only exchange expertise but also expect accountability. It means that our partners must bear a part of the security burden as well as become part of the security solution."**
>
> Michael Chertoff
> Secretary
> U.S. Department of Homeland Security

The vision for CI/KR protection involves "cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect CI/KR from terrorist attacks." Successful implementation of the NIPP to support this vision will require all government and private sector organizations involved to act together as a protective community. These security partners and their *primary* roles include:

- **Department of Homeland Security:** Overall management of the Nation's CI/KR protection framework and oversight of NIPP implementation.
- **Sector-Specific Agencies:** Implementation of the NIPP framework and guidance in designated CI/KR sectors (see table 2-1 for the designated leads for CI/KR sectors).
- **Other Federal Departments, Agencies, and Offices:** Implementation of specific roles designated in HSPD-7 or other relevant statutes and executive orders.
- **State, Territorial, Tribal, and Local Governments:** Development and implementation of a CI/KR protection program as a component of their overarching homeland security program.
- **Private Sector Asset Owners and Operators:** CI/KR protection, coordination, and cooperation.
- **Advisory Councils and Other Nongovernmental Organizations:** Insight through community-based awareness and training, workshops, and other CI/KR protection programs.
- **Regional Initiatives:** Partnerships that cross jurisdictional boundaries and focus on CI/KR protection within a defined geographic area.
- **Academia, Research Centers, and Think Tanks:** Provide CI/KR protection subject-matter expertise, independent analysis, R&D, and educational programs.

The NIPP provides the framework to support the evolving interaction among these entities to help meet new requirements and enhance existing capabilities. Organizations and coordination mechanisms facilitating the development and maintenance of public-private partnerships in support of the NIPP are discussed in Chapter 4. The roles and responsibilities of the security partners are described in more detail below.

2.1 Department of Homeland Security

As set forth in HSPD-7, DHS is responsible for managing the national CI/KR protection program. These responsibilities are discussed in the following sections organized by the NIPP objective they support.

2.1.1 Build Security Partnerships

DHS coordinates this process, and provides a single point of accountability to leverage sector-specific expertise, relationships, and resources of security partners. This involves specific responsibilities for supporting the partnership model and facilitating information exchange.

2.1.1.1 Support a Partnership Framework

- Coordinates and integrates the relationships among security partners;
- Promotes voluntary participation in CI/KR protection activities;
- Identifies market-based incentives for consideration by the executive or legislative branches of the government; and
- Provides expertise and assistance in addressing physical, human, and cyber elements of CI/KR protection.

Department of Agriculture Agriculture, food (meat, poultry, egg products)	**Department of Defense** Defense industrial base
Department of Health and Human Services Public health and healthcare (food; other than meat, poultry, egg products)	**Department of Homeland Security** Chemical (DHS/IP)
Environmental Protection Agency Drinking water and wastewater treatment systems	Commercial facilities (DHS/IP)
Department of Energy Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)	Dams (DHS/IP)
Department of the Treasury Banking and finance	Emergency services (DHS/IP)
Department of the Interior National monuments and icons	Commercial nuclear reactors, materials, and waste (DHS/IP)
	Information technology (DHS/Cyber and Telecommunications Security)
	Telecommunications (DHS/Cyber and Telecommunications Security)
	Postal and shipping (DHS/TSA)
	Transportation systems (DHS/TSA, DHS/USCG)
	Government facilities (DHS/FPS)

Table 2-1. Sector-Specific Agencies and Assigned CI/KR Sectors

2.1.1.2 Facilitate Information Exchange

- Serves as the primary Federal organization establishing the interface for information flow with security partners;
- Develops, implements, and expands information-sharing strategies and mechanisms;
- Notifies security partners on the need to take action to protect potentially high-risk assets or systems;
- Shares lessons learned and best practices on consequence and vulnerability assessment methodologies and results with security partners, as appropriate;
- Coordinates outreach efforts, in collaboration with SSAs, to security partners by providing mechanisms and processes to share information as broadly as possible;
- Maintains situational and operational awareness of CI/KR sectors to support sector-specific and cross-sector protective and response programs;
- In conjunction with the Department of State, shares appropriate CI/KR protection-related information with the international community (e.g., best practices) and performs outreach to enhance information sharing and management of international agreements regarding CI/KR protection;

- Collects information and integrates budget requirements for Federal CI/KR protection programs, and State- and local-focused programs, where appropriate;
- Offers or coordinates training and conducts exercises; and
- Maintains relationships and coordinates with Homeland Security Advisors (HSAs) and State Administrative Agencies (SAAs) to implement protection and response programs and disseminate alerts, warnings, and advisories.

2.1.2 Implement a Comprehensive, Integrated Risk Management Program

DHS provides consistent policies, approaches, guidelines, and methodologies to assist security partners in carrying out CI/KR protection activities. DHS responsibilities relative to components of the NIPP risk management framework are discussed in the following sections.

2.1.2.1 Asset and Vulnerability Identification

- In order to maintain and update an inventory and description of national CI/KR to support the identification and risk analysis DHS:
- Conducts periodic data calls to obtain information regarding national-level CI/KR focused on potentially high-risk assets;
- Incorporates information on vulnerabilities and protective actions into the national risk profile;
- Continually reviews the universe of CI/KR to identify those requiring further analysis or action in response to specific threats;
- Conducts or facilitates vulnerability assessments for selected CI/KR assets (either based on high-risk potential or specific threat information);
- Assists security partners in conducting vulnerability assessments by providing methodologies, tools, and guidelines;
- Collects, maintains, and protects information on vulnerability assessment data provided by security partners;
- Develops and distributes products such as the Characteristics and Common Vulnerabilities, and Potential Indicators of Terrorist Activity reports;
- Works with security partners to reduce vulnerabilities and minimize the severity of cyber attacks; and
- Facilitates the development, assessment, and validation of risk methodologies.

2.1.2.2 Threat Assessment

DHS integrates and analyzes law enforcement, intelligence, and other information from security partners in order to:

- Identify and assess the nature and scope of terrorist threats to CI/KR;
- Detect and identify threats to CI/KR;
- Understand threats in terms of actual and potential CI/KR vulnerabilities including those posed by natural hazards;
- Provide threat scenarios and assessments to enable vulnerability, consequence, and risk analyses;
- Provide timely analysis of current and potential terrorist activities and capabilities and disseminate pertinent information to affected security partners;

- Identify the indicators and precursors of an attack; and
- Lead the development and conduct of a national cyber threat assessment.

2.1.2.3 Cross-Sector Analysis and Prioritization

With consequence, vulnerability, and threat information provided by security partners, DHS will:

- Identify cross-sector best practices;
- Facilitate cross-sector cyber analysis by providing guidance, review, and functional cyber expertise to SSAs and other government agencies;
- Analyze for additional, unidentified dependencies, interdependencies, and cross-sector impacts;
- Assess results using statistical analysis techniques;
- Build an analytical model that integrates input from independent vulnerability, consequence, and threat analyses with a national risk scale to enable risk comparisons across sectors and regions;
- Identify potential Research and Development (R&D) needs; and
- Set national CI/KR protection priorities.

2.1.3 Implement Protective Programs

To help maximize the efficient use of resources for CI/KR protection, DHS will:

- Use prioritization results and cost and benefit analyses to inform the allocation of resources for protective programs supporting DHS and SSA requirements;
- Coordinate the implementation of protective measures for national, high-risk CI/KR;
- Develop and distribute reports detailing lessons learned or best practices for specific CI/KR asset types, such as protective measures reports;
- Conduct cost-benefit analyses for new protective programs to ensure that funding is applied where it will have the greatest effect in reducing risk; and
- Track performance measures for the CI/KR protection program and NIPP implementation process to enable continuous improvement.

2.1.4 Coordinate Cross-Sector Cybersecurity

DHS is responsible for coordinating the efforts to prevent damage, unauthorized use or exploitation of, and enable the restoration of electronic information and communications systems to ensure information confidentiality, integrity, and availability. DHS will:

- Assist SSAs in understanding and mitigating cyber risk and developing effective protective measures;
- Coordinate with other Federal agencies to provide specific warning information and protective measures and countermeasures recommendations;
- Provide technical assistance on emergency recovery plans for critical information systems;
- Coordinate the response to attacks on critical information systems; and
- Conduct and fund R&D in concert with other agencies to enable new scientific understanding and technologies in support of CI/KR protection.

2.2 Sector-Specific Agencies

SSAs provide the subject matter and industry-specific expertise and network relationships necessary to facilitate protection responsibilities within their assigned CI/KR sectors. With sector security partners, they are responsible for developing and submitting SSPs to DHS. Additionally, SSAs are required to submit annual reports to DHS including, as appropriate, activities to identify, prioritize, and coordinate CI/KR protection.

Each SSA establishes the organizational framework required to support the implementation processes outlined in the SSPs. The level of staffing and extent of expertise required varies based on the following:

- Extent of existing coordination mechanisms, regulatory processes, and assessment methodology (e.g., self-assessments or Federal-led assessments);
- Number and diversity of sector security partners;
- Data collection and storage methods;
- Number and complexity of interdependency analyses and other broad-based sector studies; and
- Degree of reliance on sector participation and DHS staff support.

SSA responsibilities that support the overarching NIPP objectives include but are not limited to the activities described in the following sections. SSAs perform these activities, as appropriate, and consistent with existing authorities, in close cooperation with security partners.

2.2.1 Maintain Security Partnerships

To support the NIPP objective of maintaining security partnerships, SSAs:

- Inventory security partners and develop contact databases for outreach efforts;
- Develop a security partner communication process that includes other SSAs;
- Support the DHS role in coordinating outreach across all CI/KR sectors;
- Establish and maintain relationships with security partners or security partner groups (e.g., through industry associations and Sector Coordinating Councils);
- Identify subject matter experts who understand the cyber aspects of their sector;
- Establish metrics and gather the required data to keep metrics current, in accordance with guidelines provided by DHS;
- Track performance measures to identify progress within the sector and provide current information to DHS;
- Provide feedback to security partners on progress and perceived gaps and weaknesses;
- Contribute to the annual DHS Critical Infrastructure Protection R&D Plan; and
- Exchange information with the international community, in accordance with guidelines established by DHS and the Department of State.

2.2.2 Implement Risk Management Programs

To support the NIPP objective of implementing risk management programs, SSAs:

- Coordinate the development, implementation, and update of SSPs;
- Work with asset owners and operators to identify CI/KR within the sector;

- Collect and store up-to-date asset data and make the necessary data accessible to DHS;
- Support sector asset information data calls from DHS;
- Establish and disseminate standards, methods, and guidance as needed consistent with DHS guidance;
- Work with DHS to evaluate or validate sector-specific risk assessment tools;
- Staff vulnerability assessment teams as needed;
- Collect, review, and warehouse self-assessment results;
- Provide assessment results to DHS;
- Increase awareness of how the business and operational aspects of the sector rely on cyber systems or processes;
- Support sector-level interdependency, consequence, and other analysis as required;
- Prioritize sector CI/KR to facilitate protective program development and implementation; and
- Provide DHS with analytical results demonstrating sector CI/KR preparedness.

2.2.3 Implement Protective Programs

To support the NIPP objective of implementing protective programs, SSAs:

- Develop and implement protective programs for high-priority CI/KR in coordination with DHS and other security partners;
- Recommend minimum standards for protective programs by asset category that may be implemented by owners or operators;
- Identify and communicate best practices for protective programs for all CI/KR;
- Conduct cost-benefit analyses for new protective programs to ensure that funding is applied where it will have the greatest effect in reducing risk;
- Allocate resources for protecting different sets of prioritized assets according to risk and agency budget appropriations;
- Ensure that planning documents include personnel and training requirements to fulfill SSA CI/KR protection responsibilities under the NIPP and NRP working bodies and operational organizations;
- Request funding to implement protective programs and plans;
- Identify regulatory options for protective measures as required and allowed by law;
- Offer training and conduct exercises as appropriate;
- Review and update existing and future sector efforts to ensure full integration of cyber awareness;
- Establish mutual assistance programs for cybersecurity emergencies;
- Report to DHS on CI/KR protection activities and progress; and
- Track performance measures for CI/KR protection and NIPP implementation process to facilitate continuous improvement.

2.2.4 Reporting

SSAs are required to provide annual reports to DHS describing sector protection efforts. These reports emphasize efforts to identify, prioritize, and protect CI/KR within the sector.

2.2.4.1 Annual

SSAs will submit an annual report for performance measurement and resource allocation purposes that:

- Describes the overall sector strategy and programs and respective links to objectives set forth in HSPD-7, the NIPP, SSPs, and other policy documents;
- Explains existing programs and capabilities in the sector, how they are funded and executed, how they are coordinated with State and local efforts, and how they address national priorities;
- Identifies sector priorities based on risk analysis;
- Provides a detailed description of resource needs for CI/KR protection;
- Tracks progress against specified CI/KR protection goals through the use of sector-specific metrics;
- Identifies gaps that exist between current and desired sector capabilities;
- Identifies best practices from successful programs;
- Includes a set of proposed programs/initiatives along with requested funding levels; and
- Provides feedback to DHS with suggestions for continuously improving the NIPP.

2.2.4.2 SSP Updates and Revisions

SSAs will review their SSPs on an annual basis to identify changes that warrant the development and issuance of a periodic update (following the same criteria presented in Section 6.5 for the Base Plan). SSPs will be revised and resubmitted to DHS on a triennial basis. Updated SSP content should include:

- Revised sector security goals tailored to guide sector activities for the next triennial cycle;
- New R&D priorities based on the emergence of developing technologies;
- Information on newly adopted protective measures;
- Descriptions of information-sharing programs and practices adopted since the last issuance of the SSP;
- Updates to sector background and other factual information as required by changing events; and
- Enhanced descriptions of activities with security partners to implement the NIPP risk management framework.

2.3 Other Federal Departments and Agencies

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal CI/KR. Federal departments and agencies are also responsible for coordinating these activities with DHS, SSAs, State and local jurisdictions, and private sector entities as appropriate. Federal departments and agencies with unique responsibilities for a particular sector that are distinct from the responsibilities of an SSA, will:

- Provide information on appropriate aspects or parts of that sector;
- Identify and assess the potential vulnerabilities and consequences for that sector;

- Play a role as the regulatory agency for owners and operators represented within that sector when so designated by statute**;** and
- Work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism.

Specific Federal departments and agencies not designated as SSAs have special functions related to CI/KR protection as follows:

- **The Department of State**, in conjunction with DHS and the Departments of Justice, Commerce, Defense, and Treasury, works with foreign countries and international organizations to strengthen CI/KR protection efforts.
- **The Department of Justice (DOJ)** reduces domestic terrorist threats, and investigates and prosecutes actual or attempted attacks on CI/KR. In addition, it has the following responsibilities specifically associated with cybersecurity:
    - Works with the Federal Trade Commission and CI/KR sectors to address barriers to mutual assistance programs for cybersecurity emergencies;
    - Works with other Federal agencies to develop and implement efforts to reduce cyber attacks and cyber threats through developing better data about victims of cyber crime and intrusions; and
    - The Federal Bureau of Investigation and intelligence community ensure a strong counterintelligence posture for cyber-based intelligence collection against the U.S. Government and commercial and educational organizations.
- **The Department of Commerce** works with DHS and private sector, research, academic, and government organizations to improve technology related to CI/KR protection.
- **The Department of Transportation (DOT)** and DHS collaborate on all matters related to transportation security and transportation infrastructure protection. DOT is responsible for operating the national air space system. DOT and DHS collaborate on regulating the transportation of hazardous materials by all modes (including pipelines).
- **The Nuclear Regulatory Commission** works with DHS to ensure the necessary protection of commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste.
- **The Intelligence Community, the Department of Defense, Department of the Interior,** and other appropriate Federal agencies collaborate with DHS to develop the geospatial program mandated by HSPD-7. The program will map, image, analyze, and sort CI/KR using commercial satellite and airborne systems, as well as existing agency capabilities.

2.4 State, Territorial, Tribal, and Local Governments

The 50 States, the District of Columbia, the Commonwealth of Puerto Rico, U.S. Territories, tribal governments, and local jurisdictions all play significant roles in the protection of the Nation's CI/KR.

2.4.1 State and Territorial Governments

State and Territorial homeland security offices are established to develop, implement, and manage their counterterrorism and CI/KR protection efforts as a component of their overall homeland security efforts. Homeland Security and Incident Management Grant program guidance includes requirements for States

and Territories to develop homeland security strategies that align to the National Preparedness Goal, thereby providing a requirement and incentive for them to address issues relating to CI/KR protection and implementation of the NIPP.

Through their CI/KR protection programs, State and Territorial government responsibilities include, but are not limited to the following:

- Identify and protect CI/KR under their control;
- Coordinate State and local jurisdiction CI/KR protection efforts to ensure compliance with and to compliment the NIPP and SSAs;
- Promote and coordinate CI/KR protection and emergency response activities among local jurisdictions, tribal entities, and regional organizations;
- Act as conduits for requests for Federal assistance when the threat exceeds the capabilities of State, Territorial, and local jurisdictions;
- Facilitate the exchange of relevant security information and threat alerts down to the local level;
- Develop and implement strategies and plans as part of the CI/KR protection program, based on the NIPP risk management framework;
- Ensure ongoing coordination with relevant international, regional, local, and private sector CI/KR protection efforts;
- Develop and implement protective measures corresponding to each level of the HSAS;
- Engage Federal, tribal, local and private sector counterparts regarding CI/KR protection initiatives through established coordination channels;
- Coordinate with DHS and other security partners to identify and characterize high-priority CI/KR protection and special events and provision of asset criticality updates based on onsite observations;
- Support or implement appropriate protective measures such as onsite presence of law enforcement, mutual aid/mutual response agreements, and public-private partnerships;
- Facilitate coordinated planning and preparedness by applying NIPP criteria for determining criticality, prioritizing protection investments, and exercising preparedness in their jurisdictions;
- Facilitate the exchange of relevant security information and threat alerts with security partners;
- Participate on relevant NIPP Government Coordinating Councils (GCC) at the request of the GCC Chairperson;
- Manage the security of computer systems while maintaining awareness of threats, vulnerabilities, and consequences to ensure that they are not used to enable attacks against CI/KR, and ensuring that local government offices and citizens manage their computer systems accordingly; and
- Establish IT security programs, including awareness, audits, and standards, and participation in established information-sharing mechanisms with other State and Territorial governments.

2.4.2 Tribal Governments

Certain tribal government roles and responsibilities overlap with those of State, Territorial, or local governments. Tribal governments also face unique challenges that are not shared by their State, Territorial, or local counterparts. As part of CI/KR protection, tribal government responsibilities include, but are not limited to, the following:

- Ensure ongoing coordination with State or Territorial CI/KR protection program on risk management efforts;
- Ensure ongoing coordination with relevant regional, local, and private sector CI/KR protection efforts;
- Engage with State or Territorial CI/KR protection program personnel to identify and protect tribal-owned CI/KR;
- Ensure tribal-owned CI/KR protective measures are included in statewide and regional efforts where appropriate;
- Develop and implement protective measures corresponding to each level of the HSAS;
- Participate as members of relevant GCCs at the request of the GCC Chairperson;
- Coordinate with DHS and other security partners to identify and characterize high-priority CI/KR and special events and provide updates on asset information based on onsite or onscene observations;
- Recognize and raise awareness regarding the unique circumstances of tribes that serve as owners and operators of CI/KR on their lands; and
- Manage the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CI/KR, and ensure that tribal government offices and tribal members manage their computer systems accordingly.

2.4.3 Local Governments

Local governments represent the front line of CI/KR protection across the Nation. Local government responsibilities include, but are not limited to, the following:

- Coordinate regularly with, and support, State and Territorial CI/KR protection programs;
- Develop and implement protective measures corresponding to each level of the HSAS;
- Engage public and private leadership in the development of coordinated local and regional plans as part of the statewide CI/KR protection program using the NIPP risk management framework to ensure the protection of residents and businesses;
- Conduct planning efforts to protect citizens and respond to emergencies;
- Ensure knowledge of communities, residents, landscapes, and existing critical services for maintaining public health, safety, and order and communicate that knowledge to appropriate security partners;
- Coordinate with DHS and other security partners to identify and characterize high-priority CI/KR and special events and provide asset criticality updates based on onsite observations;
- Participate as members of relevant GCCs at the request of the GCC Chairperson;
- Develop and implement public awareness efforts; and
- Manage the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that they are not used to enable attacks against CI/KR, and ensure that local governments and citizens manage their computer systems accordingly.

2.5 Private Sector Asset Owners and Operators

Owners and operators of CI/KR are generally the first line of defense for their own facilities and engage in risk management planning and investments in security as a necessary component of prudent business

planning and operations. These activities includes reassessing and adjusting plans, assurance, and investment programs to accommodate the increased risk posed by acts of terrorism, protect the assets under their control, and avoid adverse effects on neighboring industries and communities. Private sector owners and operators typically rely on government entities to address risks occurring outside of their property.

CI/KR protection responsibilities of specific owners or operators vary. Depending upon applicable regulations and law, responsibilities can include:

- Performing risk and vulnerability assessments;
- Undertaking a variety of protective measures to reduce identified vulnerabilities;
- Coordinating CI/KR protective measures and plans with appropriate Federal, State, and local entities;
- Assisting and supporting State and local CI/KR efforts as appropriate;
- Developing and exercising an emergency management plan and security plan;
- Participating in local government emergency management programs;
- Satisfying various cyber protection standards; and
- Establishing back-up operations that can expeditiously supplant the capacity of the damaged asset.
- Appendix G provides additional recommended practices for use by the private sector.

2.6 Advisory Councils and other Non-Governmental Organizations

Advisory councils, committees, and other organizations provide insight and play important roles in protecting the Nation's CI/KR through community-based awareness and training, workshops, and other programs.

2.6.1 CI/KR Protection Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the Government regarding protection policy and activities. These entities also help enhance public-private partnerships and information sharing. They often provide an additional mechanism to engage with a preexisting group of private sector leaders to obtain feedback on CI/KR policy and programs and make suggestions to increase the efficiency and effectiveness of government programs. Examples of advisory councils and their associated responsibilities include:

- **Homeland Security Advisory Council (HSAC):** The HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the DHS Secretary, include experts from State and local government, public safety, security and first responder communities, academia, and the private sector.
- **Private Sector Senior Advisory Committee (PVTSAC):** The Secretary of Homeland Security established the PVTSAC as a subcommittee of the HSAC to provide the HSAC with expert advice from leaders in the private sector.
- **National Infrastructure Advisory Council (NIAC):** The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all CI/KR sectors. The Council is composed of up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local government.
- **National Security Telecommunications Advisory Committee (NSTAC):** The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing

National Security and Emergency Preparedness (NS/EP) communications policy. The NSTAC is comprised of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies.

- **President's Information Technology Advisory Committee (PITAC):** The PITAC provides the President, Congress, and Federal agencies involved in information technology R&D with expert, independent advice on maintaining America's preeminence in advanced information technologies, including such elements of the national CI/KR as high-performance computing, large-scale networking, and high-assurance software and systems design.

2.6.2 Other Organizations

Many other national-level organizations are either chartered or have dedicated working groups or affiliations to support CI/KR protection. The following are representative of such organizations:

- **Interagency Security Committee (ISC):** A permanent body established to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States that are occupied by Federal employees for nonmilitary activities.
- **FBI InfraGard:** A public-private sector partnership that educates the public on CI/KR protection (via trainings/presentations), disseminates information through the InfraGard network, and provides preventive information and a forum for government and private sector interaction. In addition, InfraGard has created Sector Chief Representatives as a direct point of contact to build member relationships and facilitate more information sharing and input from/to its constituent membership.

2.7 Regional Initiatives

Regional initiatives include public-private partnerships that cross jurisdictional boundaries and focus on preparedness within a defined geographic area. These initiatives are unique to regional geography, security partners, and sector interests. Specific regional initiatives range in scope from organizations that include multiple jurisdictions in a single State to groups that involve jurisdictions in more than one State and across international borders. In many cases, State governments also will collaborate through the adoption of interstate compacts to formalize a partnership regarding CI/KR protection activities.

Although regional initiatives are not assigned responsibilities under the NIPP, many of their component members are. Directors of individual regional initiatives are encouraged to capitalize on the area-specific expertise and influence to:

- Encourage collaboration among security partners in implementing NIPP activities;
- Facilitate education and awareness of CI/KR protection efforts occurring within their geographic area;
- Coordinate regional exercise and training programs including a focus on CI/KR interdependencies and protection collaboration across jurisdictional boundaries;
- Work with State, Territorial, tribal, and local governments, and the private sector to evaluate regional CI/KR interdependencies;
- Conduct planning efforts, in coordination with their constituents, to protect citizens and enable timely response to emergencies;
- Facilitate information sharing between and among their members;
- Establish intra- and extra-regional communication mechanisms that other NIPP security partners can engage in or contribute to;

- Work with government at all levels to ensure a common understanding of risk within the region and contribute to ongoing preparedness activities; and
- Assess the CI/KR protection efforts occurring within the region to determine if any critical gaps exist and work with regional partners to remedy these gaps.

The Steering Committee of the cross-regional coordinating body, the *National Homeland Security Regional Initiative*, is responsible for representing the interests of all the regional initiatives at the national level in coordination with DHS to examine options for encouraging new regional initiatives, and exchanging information on best practices, emerging issues, accomplishments, and progress.

2.8 Academia, Research Centers and Think Tanks

The academic, research, and think tank community provides expertise and has the following roles in protecting the Nation's CI/KR:

- Establish Centers of Excellence to provide independent analysis of CI/KR protection issues;
- Advance the development, testing, evaluation, and deployment of CI/KR protection technologies;
- Establish information-sharing mechanisms to address attacks and vulnerabilities;
- Analyze, develop, debate, and share best practices related to CI/KR protection efforts;
- Research and provide innovative thinking and perspective on threats and the behavioral aspects of terrorism;
- Provide model guidelines empowering Chief Information Officers to address cybersecurity;
- Develop best practices for IT security;
- Develop and provide suitable security risk analysis and risk management courses for CI/KR protection professionals; and
- Conduct research to identify new technologies and analytical methods that can be applied by security partners.

3 The Protection Program Strategy: Reducing Risk

The cornerstone of the NIPP is the risk management framework. This framework (see figure 3-1, below) establishes the process for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk that drives CI/KR risk-reduction activities. The framework applies to the general threat environment as well as to specific threats or incident situations.

This chapter addresses the application of the risk management framework as part of the overall effort to ensure a "steady-state" of protection within and across each of the CI/KR sectors. DHS and the SSAs share responsibilities for implementing the risk management framework. SSAs are responsible for leading sector-specific risk-reduction programs and for ensuring that the sector-specific application of the risk management framework is addressed in their respective SSPs. DHS supports these efforts by providing guidance, tools, and analytical support to SSAs and others. DHS is also responsible for leveraging the results obtained in sector-specific risk management efforts to support cross-sector risk analysis and management. This includes the assessment of interdependencies and cascading effects, identification of common vulnerabilities, development and sharing of common threat scenarios, establishing and implementing cross-sector measures to reduce risk, and identification of specific R&D needs.

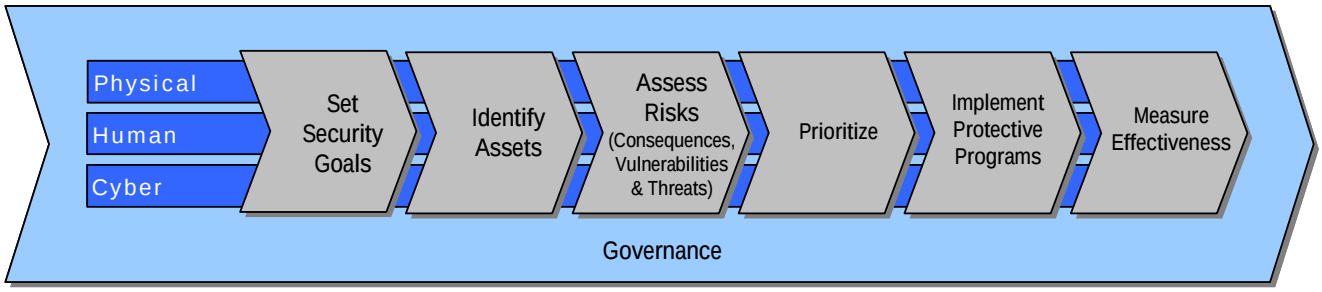


Figure 3-1. NIPP Risk Management Framework

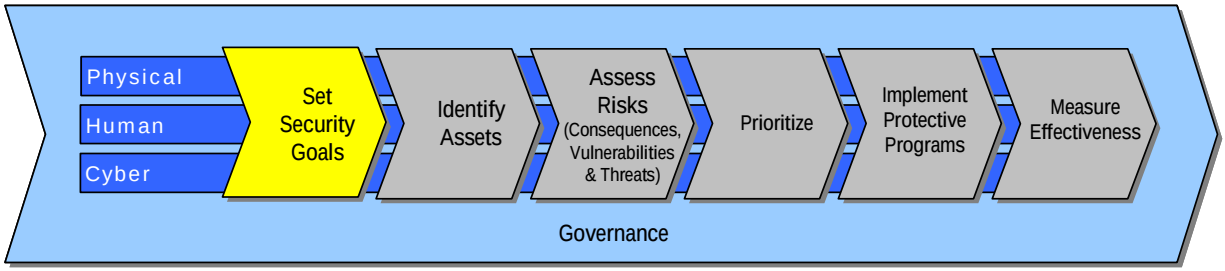
The NIPP risk management framework includes the following specific activities:

- **Set security goals:** Define specific outcomes, conditions, end points, or performance targets that collectively represent an effective security posture.
- **Identify assets:** Develop an inventory of the individual assets and systems that make up the Nation's CI/KR, some of which may be located outside the U.S., and collect information on them, including dependencies, interdependencies, and reliance on cyber systems.
- **Assess risks:** Determine which assets and systems are critical by calculating risk, combining potential direct and indirect consequences of an attack (including dependencies and interdependencies associated with each identified asset), known vulnerabilities to various potential attack vectors, and general or specific threat information.
- **Prioritize:** Aggregate and order assessment results to present a comprehensive picture of national CI/KR risk in order to establish protection priorities and provide the basis for planning and the informed allocation of resources.
- **Implement protective programs:** Select appropriate protective measures or programs and allocate funding and resources designed to address targeted priorities.
- **Measure effectiveness:** Incorporate metrics and other evaluation procedures at the national and sector levels to measure progress and assess effectiveness of the national CI/KR protection program.

DHS uses information resulting from metrics and other evaluation procedures as part of the final step of the risk management framework to support a constant feedback loop. This allows the Federal Government and its security partners to continuously refine the national CI/KR protection program in a dynamic process, thus maximizing the ability to efficiently achieve the NIPP goals and objectives described in Chapter 1.

Using the risk management framework described above, it is important to consider the physical, human, and cyber elements of an infrastructure or resource during each step of the risk management process. In addition, overarching coordination and management activities that are part of governance are the foundation of successful implementation of a national risk reduction program. DHS is responsible for the overall management of NIPP governance activities.

3.1 Set Security Goals



Achieving a secure, protected, and resilient infrastructure requires a common set of national and sector-specific security goals that collectively represent a desired security posture. These goals should consider the physical, human, and cyber elements of CI/KR protection. Security goals will vary across and within sectors, depending on the internal structure and composition of a specific industry, resource, or other aspect of CI/KR.

Nationally, the overall goal of risk-reduction efforts is an enhanced state of CI/KR protection achieved through the implementation of focused risk-reduction and protective strategies within and across sectors. The risk management framework supports this goal by:

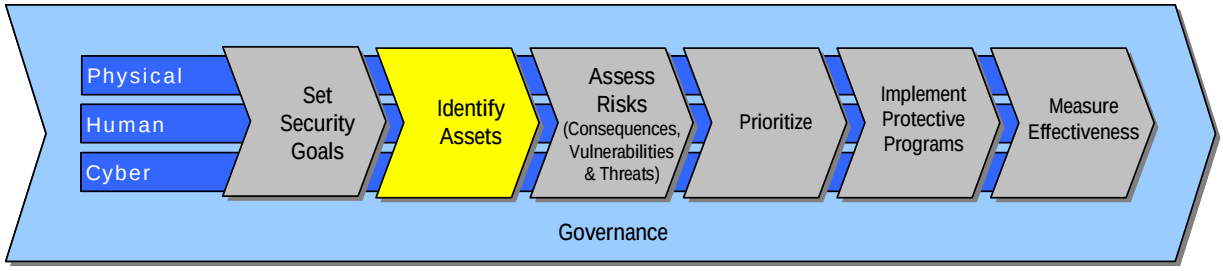
- Informing the national risk profile to include a high-level snapshot summary of the aggregate risk and the protective status of all sectors. The national risk profile is developed by DHS in collaboration with other security partners, updated on an ongoing basis, and used to support strategic decisionmaking and resource allocation.
- Enabling DHS and SSAs to determine the best course of action to reduce potential consequences or vulnerabilities. Depending in part on existing statutory authorities, some available options include encouraging voluntary implementation (e.g., through public-private partnerships), pursuing incentive-related policies and programs, or undertaking regulatory action.
- Using prioritized information to create, or identify, specific protective programs for CI/KR of highest criticality based on risk. Depending on the protective program, resource allocation may occur at the Federal, State, Territorial, tribal or local level, or may be solely the responsibility of asset owners and operators. International outreach and collaboration also may be required under certain circumstances.

From a sector perspective, security goals:

- Define or illustrate the protective posture (physical, human, and cyber) that security partners seek to attain;
- Consider distinct assets, systems, operational processes, business environments, and risk management approaches; and
- Vary according to the characteristics and security landscape of the affected sector, State, Territory, or region.

Taken collectively, these goals guide all levels of government and the private sector in tailoring protective activities to address CI/KR protection needs.

3.2 Identify Assets



Once security goals are set, the next step is to develop and maintain a comprehensive inventory of the Nation's CI/KR within and outside our borders.

The process for identifying nationally critical assets involves a comprehensive approach that considers the physical, human, and cyber elements of an asset or system. The approach includes gathering information on the relationships (e.g., dependencies and interdependencies) between various assets and systems to help develop a more complete picture of the national CI/KR. It also includes working with international partners to gather information on the foreign infrastructure and resources upon which U.S. CI/KR rely.

The NIPP defines an infrastructure asset as something of importance or value belonging to one of the 17 CI/KR sectors that if targeted and exploited, destroyed, or incapacitated could result in large-scale injury, death, economic damage, or destruction of property, or could profoundly damage the Nation's prestige and confidence. Assets include one or more of the following elements:

- **Physical elements:** Tangible property such as facilities, components, real estate, animals, and products.
- **Cyber elements:** Electronic information and communications systems and the information contained in those systems, and comprising all the hardware and software that processes (i.e., creates, accesses, modifies, and destroys), stores (i.e., all media types: paper, magnetic, and electronic), and communicates (i.e., shares and distributes) information, or any combination of all of these elements.
- **Human or living elements:** Critical knowledge or functions of people (i.e., job expertise or skills) uniquely susceptible to attack.

A comprehensive inventory of the Nation's CI/KR is being developed through a collaborative effort between Federal, State, Territorial, tribal, and local, governments, and the private sector, and will be used to frame national CI/KR risk management efforts.

3.2.1 National Asset Inventory

DHS maintains and is enhancing a comprehensive catalog that includes an inventory and descriptive information regarding the assets and systems that comprise the Nation's CI/KR. This National Asset Database (NADB) allows for the analysis of consequences, specific and common vulnerabilities, dependencies, and interdependencies, both within and across sectors and geographic regions.

SSAs have worked extensively with DHS to ensure that the NADB data framework accurately represents each sector. In addition, the NADB includes a cyber data framework to characterize each sector's unique cyber assets or systems.

Information for the NADB comes from a variety of sources:

- **Sector inventories:** SSAs provide and update inventories on a periodic basis to ensure that sector assets are adequately represented, and that sector and cross-sector dependencies and interdependencies can be identified and analyzed.
- **Periodic data calls:** DHS conducts periodic data calls with security partners requesting that they voluntarily provide detailed information on infrastructure within their purview.
- **Voluntary submittals from security partners:** Owners and operators, State, Territorial, tribal, and local governments, and Federal departments and agencies may submit information on assets for DHS to consider for inclusion in the NADB at any time.
- **Results of prior studies:** Various studies undertaken by trade associations, advocacy groups, and regulatory agencies have been used to identify and gather data on infrastructure.
- **Ongoing reviews of particular locations where threats are focused:** DHS- and SSA-initiated site assessments provide information on vulnerability, help to identify assets and their dependencies and interdependencies, and quantify asset value related to potential consequences resulting from an attack.

In coordination with SSAs and asset owners, basic information, such as name, location, owner and function, will be gathered for all assets regardless of consequentiality. Additional information is gathered for assets that DHS determines to be of national significance based on an initial screening, including:

- System components that are central to the infrastructure mission and function;
- Dependencies and interdependencies (what the asset depends on in order to function, and what assets are reciprocally dependent upon it);
- Continuity, redundancy (including backups), and resiliency built into the asset;
- Existing protective measures (e.g., fencing, biometrics, firewalls); and
- Worst reasonable case consequences (that would result if the asset were destroyed, incapacitated, or exploited) including:
- Sufficient information about the asset or system to conduct quantitative consequence analysis using methodologies existing or under development;
- Quantitative consequence assessment information with supporting documentation to enable further normalization of data and comparative risk analysis provided by the SSA, private sector, or other subject-matter expert.

3.2.2 SSA Roles in Asset Identification

SSAs serve as the primary conduit between government and industry and can facilitate awareness of the need to identify assets and promote and support sector-, regional- and national-level data collection

efforts. The processes that SSAs use to collect asset data and coordinate with DHS are described in the individual sector-specific annexes to the NIPP along with descriptions of mechanisms for making data collection efforts more manageable, such as:

- Prioritizing the approach for reaching out to different security partners;
- Identifying assets of potential national-, regional-, or sector-level importance;
- Identifying, reviewing, and using existing databases; and
- Identifying specific assets, or classes of assets, for which additional data collection is unnecessary because of the inherently low risk associated with a potential terrorist attack.

SSAs identify and obtain data for all CI/KR that play a vital role in the Nation's security or economy—particularly when dependencies or interdependencies are recognized or discovered. For example, a small manufacturer of pharmaceuticals or vaccines could be the sole U.S. manufacturer of that product. Similarly, a small plant could be the primary producer of a component vital to the defense industrial base. The identification of less visible assets makes the effort more time-consuming, but is a crucial part of the process if a true national risk profile is to be developed.

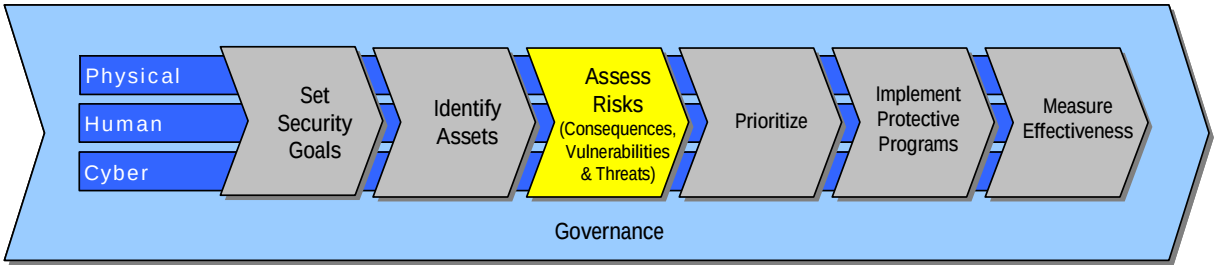
3.2.3 Identifying Cyber Assets

Cyber assets represent a variety of hardware and software components, whereas cyber systems are a set of cyber assets that interact to perform a particular function. Cyber assets and systems should be identified individually or included as a cyber element of a physical asset or system's description if they are associated with one. The following list provides examples of cyber assets or systems that exist in most, if not all, sectors:

- Automated access control systems supporting physical access control;
- Digital control systems including Supervisory Control and Data Acquisition (SCADA) systems and Process Control Systems (PCS); and
- System interconnections (i.e., trusted connections) defined as the direct connection of two or more IT systems owned by separate organizations.

DHS is developing a cross-sector cyber asset identification methodology that, when applied, would enable a sector to identify cyber assets and characterize the reliance of a sector's business and operational functionality. If a sector already has developed and is employing a cyber asset identification methodology, DHS will work with the sector to ensure alignment of that methodology with the NIPP risk management framework.

3.3 Assess Risks



A variety of methodologies are available across the CI/KR sectors to assess risk. However, a common approach is needed so that DHS and its security partners can set CI/KR protection priorities across the CI/KR sectors. The first step toward achieving that common approach is to establish a common definition and analysis of the basic factors of risk:

- **Consequence analysis:** Estimates the damage that a successful attack would cause.
- **Vulnerability assessment:** Identifies weakness in an asset or system's design, implementation, or operation that can be exploited by an adversary.
- **Threat analysis:** Estimates the likelihood that a particular target, or type of target, will be selected for attack. In the context of risk, threat likelihood is based on the analysis of the intent and capability of an adversary.

When these three factors are combined, they form the risk associated with an asset or system (i.e., the potential for loss of or damage to an asset or system). Risk can be calculated for an asset, system,[2] or set of assets or systems. The result is a comprehensive, systematic, and defensible assessment of asset, system, sector, or national risk that drives integrated risk-reduction activities.

To ensure that the risk assessment methodologies used in individual sectors result in data that can be compared within and across sectors, SSAs are required to align assessment products with the common approaches, standards, and guidelines established by DHS for measurement or assessment of consequences, vulnerabilities, and threat, and the calculation of risk. Where existing assessment tools do not conform to DHS guidelines, sectors must either work with DHS to normalize their risk assessment results or adopt the tools that have been developed by DHS for this purpose. These approaches and guidelines are discussed in greater detail in Appendix C.

To help ensure the comparability of risk-related measurements, DHS is developing a suite of tools called Risk Analysis and Management for Critical Asset Protection (RAMCAP). This tool set will enable owners and operators to calculate potential consequences and vulnerability to an attack using a consistent system of measurements, as well as the means to convert and compare the results obtained from prior assessments performed with certain approved methodologies. By helping standardize these ranked factors, RAMCAP will enable detailed and rationalized cross-sector analysis. DHS is working with security partners to develop, implement, and validate RAMCAP consequence and vulnerability assessment methodologies for each of the CI/KR sectors.

[2] A system is a collection of resources or elements made up of any combination of functions, physical attributes, or cyber components that perform a process.

3.3.1 Consequence Analysis

The first factor to be considered when assessing risk is the potential consequences associated with a successful attack. In the context of a terrorist attack on a CI/KR asset or system, consequence is generally measured as the range of loss or damage that can be expected from a successful attack. Pursuant to HSPD-7, consequences of national significance[3] include those that could:

- Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- Impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
- Undermine State and local government capacities to maintain order and to deliver minimum essential public services;
- Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- Have a negative effect on the economy through the cascading incapacitation of other CI/KR; or
- Undermine the public's morale and confidence in the national economic and political institutions.

DHS will work with security partners to examine inherent characteristics of assets or systems to identify the worst reasonable case consequences that are likely to result if the asset is destroyed, incapacitated, or exploited. In order to support a comparative risk analysis, it is important for security partners to use common terminology and metrics when assessing consequences, and to express the results in terms of comparable units. To enable this, DHS is working with security partners to develop consequence assessment methodologies that can be applied to a variety of asset or system types and produce comparable quantitative consequence estimates. Specifically, DHS is working with the American Society of Mechanical Engineers and various industry partners to develop RAMCAP consequence assessment methodologies for various CI/KR sectors and subsectors. When fully developed and implemented, the RAMCAP methodologies will provide quantitative results that can be compared to the results of any other RAMCAP consequence assessment, regardless of asset type.

While use of the RAMCAP methodologies is encouraged, it is acknowledged that satisfactory consequence assessments were performed on numerous assets and systems prior to the advent of RAMCAP. RAMCAP is being designed to leverage the use of these earlier efforts so that results obtained using robust methodologies with certain common characteristics can support the national cross-sector analysis with minimal or no additional effort required on the part of asset owner/operators.

Consequence analysis should not be limited to direct effects. Many assets depend on multiple inputs to maintain functionality. For example, nearly all sectors rely on the energy, information technology, telecommunications, banking and finance, and transportation sectors. In some cases, a failure of an asset in one sector will have a significant impact on the ability of an asset in the same or another sector to perform the necessary functions. This reliance on another asset or sector for functionality of certain assets is called a ***dependency***. If two assets depend on one another, then they are ***interdependent***.

Various Federal, State, Territorial, tribal and local entities, including national laboratories, are engaging in the development of sophisticated models and simulations to identify linkages within and across sectors. The U.S. Government established the National Infrastructure Simulation and Analysis Center (NISAC) in support of this effort. The NISAC charter is to develop advanced modeling, simulation, and analysis

[3] Paragraph (7), sections (a) through (f) of HSPD-7.

capabilities of the Nation's CI/KR and their physical and cyber cross-sector dependencies and interdependencies in an all-hazards context (natural, accidental, and malevolent). NISAC will improve the Nation's understanding of infrastructure dependencies and interdependencies, and better inform decisionmakers in the areas of policy analysis, investment, prevention and mitigation planning, education, training, and crisis response.

The level of granularity achieved by using sophisticated models and simulations is neither realistic nor necessary for all assets, systems, or sectors. In many circumstances, a simplified dependency and interdependency analysis is sufficient to provide the insight necessary to make informed risk management decisions.

3.3.2 Vulnerability Assessment

The second factor to be considered when assessing risk is vulnerability. Vulnerabilities are the characteristics of, or flaws[4] in, an asset or system's design, location, security posture or operation that render it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards.[5] Vulnerability assessments are systematic measurements of the susceptibility of a sector, segment, region, individual asset or system to an attack. They identify areas of weakness that could result in consequences of concern, taking into account intrinsic structural weaknesses, protective measures, and redundancies. Vulnerability assessments typically consist of the following key elements:

- Determine an appropriate vulnerability assessment strategy (e.g., self-assessment, State- or Federally led assessment, expert reviews, or third-party assessment);
- Identify a methodology/tool appropriate for the particular type of asset at hand;
- Identify and group vulnerabilities using common threat scenarios;
- Identify dependencies and interdependencies with other assets and sectors;
- Consider vulnerabilities associated with physical, human, and cyber elements;
- Analyze benefits of existing protective programs; and
- Assess residual gaps to determine unresolved vulnerabilities.

Dozens of different vulnerability assessment methodologies exist and are being used by security partners in the CI/KR sectors. The vulnerability assessment methodologies to be used within each sector are described in the respective SSPs. The SSPs also describe in general terms how the assessments are to be carried out (e.g., by whom, how often).

In order to support comparative risk analysis across sectors, the results of vulnerability assessments must be comparable. To ensure this comparability, DHS is developing RAMCAP Security Vulnerability Assessment (SVA) modules for use in multiple sectors and subsectors. The RAMCAP SVA modules use a common approach to produce assessment results that can be compared with other RAMCAP SVA module assessment results regardless of the asset or system type being assessed. It also allows the use of results from vulnerability assessments performed using other assessment methodologies that have certain characteristics in common with the RAMCAP SVA methodology.

---

[4] Vulnerabilities may also be present as flaws in security procedures, software, internal system controls, or the design and use of an information or communication system that may affect the confidentiality, integrity, or availability of the system or the information contained therein.

[5] While the programs and processes in the NIPP are focused on enhancing CI/KR protection in light of terrorism and security challenges, they have a broad applicability to all-hazards.

SSAs are responsible for facilitating vulnerability assessments (which are typically performed by asset owners or operators) within their sectors and gathering the vulnerability assessment results for use in sector and national risk management efforts. If a methodology other than the RAMCAP SVA module is used, SSAs must ensure that the outputs of the assessments performed on their sector's assets conform to DHS minimum standards and allow for comparison of results within and across sectors.[6] In addition, SSAs are responsible for validating the results of assessments at assets that are of the greatest concern from the sector perspective. For these assets, SSAs should participate in conjunction with the asset owner in the conduct or review of the vulnerability assessment.

DHS is responsible for ensuring that comprehensive vulnerability assessments are performed for CI/KR of national significance. This may involve DHS experts performing the vulnerability assessment in conjunction with the asset owner or operator, or a third party auditor, or simply working with the asset owner or operator or third party auditor to validate the results of the assessment.

DHS also conducts or supports vulnerability assessments to:

- More fully investigate dependencies and interdependencies within and between sectors;
- Serve as a basis for developing common vulnerability reports that can help to identify strategic needs for protective programs or R&D across sectors or subsectors;
- Fill selected gaps when sectors or asset owners or operators have not yet completed assessments and such studies are needed immediately; and
- Test and validate new methodologies or streamlined approaches for assessing vulnerability before making them generally available to security partners.

In some sectors and subsectors, vulnerability assessments have never been performed or have been performed for only a small number of high-profile or high-value assets or systems. To help close this gap, DHS will provide the following assistance to security partners:

- Help to determine the common criteria for vulnerability assessments, particularly for nationally critical assets and systems;
- Provide vulnerability assessment tools to be used as part of the self-assessment process;
- Provide Characteristics and Common Vulnerabilities reports and Potential Indicators of Terrorist Activity reports for industrial sectors, classes of activities, and high-consequence or at-risk special event sites;[7]
- Provide references of generally accepted risk assessment principles for major classes of activities and high-consequence or at-risk special event sites;
- Help to oversee the development and sharing of industry-based standards and tools;
- Suggest the frequency of assessments, particularly in light of emergent threats;
- Conduct site assistance visits and perform vulnerability assessments of specific CI/KR of particular concern; and
- Disseminate cross-sector cyber vulnerability assessment best practices.

[6] Recommended standards and characteristics for a robust vulnerability assessment methodology are discussed in greater detail in appendix C.

[7] See section 3.5 for a discussion of these reports.

3.3.3 Threat Analysis

The final input to the risk formula is the assessment of threat, or the likelihood of a terrorist attack, on a particular asset or system. Although SSAs and sector security partners are uniquely qualified to analyze CI/KR consequences and vulnerabilities, analysis of the current terrorist threat to the United States is derived from extensive study and understanding of terrorists and terrorist organizations and is dependent on analysis of classified information. DHS will provide U.S. Government-coordinated assessments of potential terrorist threats derived from analysis of adversary intent and capability. These threat assessments will include postulated terrorist attack methods and discuss what is known about terrorist interest in particular infrastructure sectors. Since international terrorists have continually demonstrated flexibility and unpredictability, DHS will frame known terrorist goals and collective capabilities to provide CI/KR owners and operators with a broader view of the potential threat.

Threat analysis for CI/KR is produced by the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). Responding to direction in section 201 of the Homeland Security Act of 2002, DHS created an organization to bring together intelligence and infrastructure specialists to facilitate a complete understanding of the risks to U.S. CI/KR. By combining analysis of all available threat intelligence and trends analysis with expert knowledge of U.S. CI/KR, vulnerabilities, potential consequences of attacks, and resulting protective actions, HITRAC develops robust analytical products that draw actionable conclusions regarding threats and risks to the Nation's infrastructure. In the process, it identifies and refines intelligence collection requirements so that the intelligence community can better support the national CI/KR protection mission.

3.3.3.1 Threat Analysis Tools and Information

HITRAC will provide three types of threat analyses to support the NIPP. The first two provide tools intended to assist risk assessment, while the third is a commitment to report on the current terrorist threat to U.S. CI/KR:

- **Common Threat Scenarios:** The threat scenarios provided for the NIPP are descriptions of potential attack methods based on known or desired terrorist capabilities. These scenarios, which will be updated as needed, are detailed vignettes of the methods terrorists might use to attack the U.S. infrastructure and are derived from study of terrorist intentions and capabilities. These scenarios are intended to inform vulnerability and consequence analyses while ensuring that a given risk analysis has taken into account the minimum set of potential attack vectors and the associated vulnerabilities and consequences.

- **General Threat Environment:** HITRAC will work with the private sector to provide sector- and subsector-specific threat products. These products will include known specific and general terrorist threat information for each sector and will be updated on a routine basis as intelligence developments warrant. Additionally, HITRAC will produce longer-term strategic assessments and trends analysis of the evolving threat to the Nation's CI/KR. This analysis and other specialized products are designed to inform SSP developmental and operational planning, and resource investment on the part of the private sector and government. Since the probability of any threat actually materializing is uncertain, security partners must employ a risk management approach and adopt a balanced response to the range of possible or probable threats. DHS must provide threat assessments to SSAs or CI/KR owners and operators in a manner conducive to risk analysis. To assist with this requirement, HITRAC has developed an analytical tool for identifying which sectors are prone to various types of attack based on terrorist attack objectives, and has captured this information in the Terrorist Strategic Target Selection Matrix. This matrix is based on intelligence analysis that considers the three major terrorist motives for attacks on the United States.

- **Specific Threat Information:** HITRAC monitors real-time intelligence streams to provide intelligence-infrastructure fusion analysis of developing threat information. These analyses can include new information on targeted locations, sectors, or assets; new attack methods; or potential timing of an attack. If warranted, the subsequent increase in the tactical threat level will drive short-term protective measures to reduce risk. Specific threat information will inform the analysis of the general threat environment and the periodic updating of the common threat scenarios.

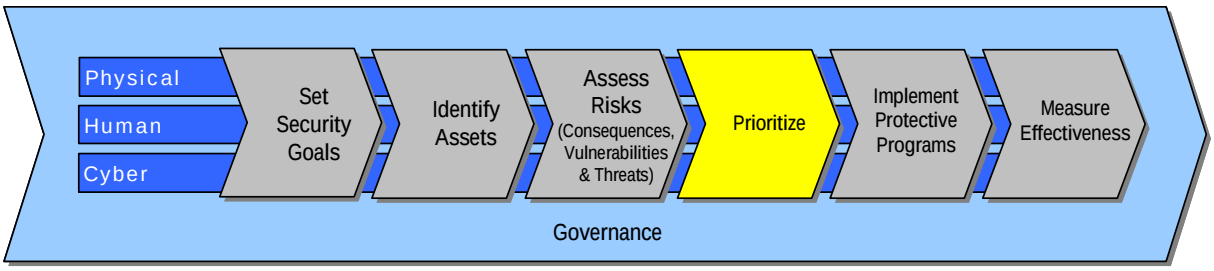
3.3.3.2 Use of Threat Analysis in Risk Assessment

To frame the full range of potential terrorist targets, DHS has assembled available data regarding international terrorist goals, objectives, and attack capabilities. This data, in turn, is mapped against CI/KR that would best suit a given terrorist attack profile. This presents analysts, decisionmakers, and owners and operators conducting risk analysis with as broad a picture of possible threats as practical, based on what is known about terrorists, absent any specific knowledge of actual target selection.

This analysis is provided in the Terrorist Strategic Target Selection Matrix, which is updated and distributed as a stand-alone document on a routine basis by HITRAC as one of its General Threat Environment analysis products. Based on in-depth intelligence analysis, the matrix arrays attack methods (in columns) against the CI/KR sectors and their primary sub-sectors (in rows). It specifies which of the principal terrorist objectives would be attained through each attack method for each specific sector and sub-sector. Attack/sector combinations are left blank in the matrix when intelligence analysis has determined that terrorists are unlikely to use a particular attack method against a specific CI/KR sector or sub-sector because terrorists' objectives cannot be achieved with such an attack. Attack/sector combinations that only meet a few of the primary terrorist attack objectives, and thus would not be as attractive a target as other CI/KR attacks, are reported as subject to a reduced threat of attack.

Sector/attack combinations that are blank in the matrix do not require further risk analysis because intelligence-based assessments indicate that these combinations are unlikely to warrant terrorists' time and resources. When combined with consequence analysis, this focuses subsequent vulnerability analysis on those combinations where there may be a high return for protection program investments or a substantial payoff for protection initiatives.

3.4 Prioritize



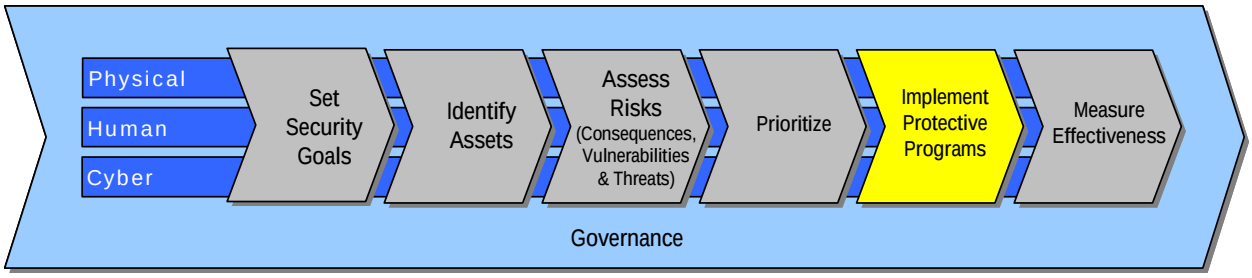
After risk-related data have been collected, the results of the risk assessments are prioritized to help identify where a risk-reduction focus is most pressing, and subsequently determine what protective actions should first be targeted. Prioritization requires a comparison of the relative levels of asset and sector risks within the context of options for achieving the established security goals.[8] Differences in the sector assessment methodologies and characterizations of risk often result in significant differences in the

[8] The prioritization of assets by risk is used to determine *where* resources should be applied first, while once assets are prioritized, cost-benefit analyses are performed on proposed protective measures to determine *how* limited resources should be allocated. Refer to chapter 7 for additional detail on resource allocation.

consistency and comparability of risk data. The process of transforming risk data into comparable units is called *normalization*.

Currently, DHS uses simple analytical normalization tools to convert risk assessment results into comparable units. Ideally, in the future, the assessment tools used within the different sectors will produce results in a comparable manner, thus precluding the need to perform translations or conversions to complete the normalization process. The RAMCAP methodologies being developed by DHS in conjunction with private industry will produce results in such a manner, allowing risk-based comparisons of assets from different sectors without application of a separate normalization step. The RAMCAP methodologies will also include means for sectors to convert results derived using legacy methodologies to the RAMCAP standardized approach. Where such mapping is not possible, DHS will encourage a sector to migrate to RAMCAP or other more standardized analytical tools to measure risk.

3.5 Implement Protective Programs



Security partners implement protective actions and programs within and across sectors. The highly distributed nature of CI/KR (physically and logically) generally means distributed ownership and execution of protection programs, but also requires centralized leadership to drive consistent implementation and ensure the greatest return on investment.

3.5.1 Protective Actions

Protective actions may involve measures designed to prevent, deter, and mitigate terrorist attacks on CI/KR assets, as well as to protect an asset if it is attacked and respond to and recover from such attacks in a manner that limits the consequences. Protective actions attempt to indirectly affect the threat and directly affect the vulnerability and consequence of a CI/KR asset as follows:

- **Deter:** Cause the potential attacker to perceive that the risk of failure is greater than that which they find acceptable. Examples include improved awareness and security (e.g., restricted access, vehicle checkpoints), and enhanced police presence.
- **Devalue:** Reduce the attacker's incentive by reducing the target's value. Examples include developing redundancies and backup systems or individuals, or deemphasizing the importance of particular special events.
- **Detect:** Identify potential attacks and validate and/or communicate the information as appropriate. General detection activities include intelligence gathering, analysis of surveillance activities, and trend analysis of law enforcement reporting. For specific assets, examples include intrusion-detection systems, network monitoring systems, operation alarms, surveillance, detection and reporting, and employee security awareness programs.
- **Defend:** Protect assets by preventing or delaying the actual attack, or reducing an attack's affect on an asset. Examples include perimeter hardening through enhancing buffer zones, fencing, structural integrity, and cyber defense tools such as antivirus software.

Protective programs also may include actions that have an impact on the consequences should an attack occur. These actions are focused on the following aspects of preparedness:

- **Mitigate:** Lessen potential impacts of an attack, such as introducing system redundancies, reducing asset dependency, or isolating downstream assets (e.g., the use of firewalls in information systems).
- **Respond:** Designed to enable rapid reaction and emergency response to an attack, such as conducting exercises and having adequate crisis response plans, training, and equipment.
- **Recover:** Allow the sector to resume operations quickly and efficiently, such as developing continuity of operations plans.

In situations where robustness and resiliency are keys to CI/KR protection, providing protection at the system level rather than the asset level may be more effective and efficient.

3.5.2 Characteristics of Protective Programs

Effective protective programs are comprised of specific protective actions and have the following characteristics:

- **Comprehensive:** Effective protective programs must address the physical, human, and cyber elements of CI/KR and consider long-term, short-term, and sustainable activities. SSPs describe programs and initiatives to protect assets within the sector (e.g., operational changes, physical protection, equipment hardening, backup communications, response plans, and security system upgrades).
- **Coordinated:** Because of the highly distributed and complex nature of CI/KR sectors, the responsibility for protecting assets must be coordinated:
    - Asset owners and operators (public or private) have an inherent responsibility to protect property, information, and people, minimally through increased awareness of terrorist threats and simple operational responses to reduce vulnerability (e.g., changing daily routines and keeping computer software and virus checking applications up to date).
    - State, Territorial, tribal, and local entities are involved in the development of protective programs, supplement Federal guidance and expertise, and provide specific law enforcement personnel as needed.
    - SSAs provide information on the most effective long-term protective strategies and coordinate the development and implementation of protective programs. For some sectors, this includes the development and sharing of standards and criteria, guidance documents, and tools.
    - DHS, in collaboration with other public and private sector partners, serves as the national focal point for the development and implementation of protective programs (including cyber-security efforts) for high-risk assets.
- **Risk-Based:** Protective programs focus on reducing risk by specifically affecting elements of consequence and/or vulnerability. Protective actions should be designed to allow measurement and evaluation. This allows asset owners and operators, and SSAs to reevaluate risk after the program has been implemented as well as to measure the effect on sector security.
- **Cost-Effective:** Effective protective programs seek to minimize excessive costs by focusing on protective actions that, among other things:
    - Employ simple, low-cost measures whenever possible;

- Are consistent with best business practices and are shared among security partners using industry and trade association communication mechanisms;
- Contain cost-sharing incentives, market systems, and other methods for encouraging private sector action;
- Build on current efforts that have proven to be effective;
- Are broadly applicable, but allow owners and operators to select the measure best suited to the particular need;
- Rely on self-assessments, where appropriate; and
- Are proportional to the risk.

3.5.3 Protective Programs, Initiatives, and Reports

DHS has developed various programs and initiatives that are intended to reduce CI/KR risk at the national level. Examples of DHS-supported activities are described in the following sections.

3.5.3.1 Protective Programs and Initiatives

- **Buffer Zone Protection Program (BZPP):** The BZPP is a grant program designed to provide resources to State, Territorial, and local law enforcement (LLE) and other security professionals to enhance security "outside the fence" of CI/KR, thereby making it more difficult for terrorists to conduct surveillance or successfully launch an attack from the immediate vicinity of a potential target. As part of the BZPP, DHS provides training on developing facility-specific Buffer Zone Protection Plans that:
  - Define a buffer zone outside the security perimeter of a specific CI/KR;
  - Identify specific threats and vulnerabilities associated with the CI/KR and the buffer zone through vulnerability assessments typically conducted by LLE officers trained by DHS; and
  - Recommend protective measures for application in or related to the buffer zone that would be most effective in devaluing the CI/KR, deterring an attack, detecting an aggressor, and defending against an attack.

  Implementation of the Buffer Zone Protection Plan results in an increase in asset and community protection and preparedness by:
  - Developing Vulnerability Reduction Purchasing Plans (VRPPs) that identify equipment needed by LLE to protect these assets effectively;
  - Providing LLE with the financial resources necessary to execute approved VRPPs; and
  - Verifying and validating that equipment purchases adequately mitigate vulnerabilities identified in the individual Buffer Zone Protection Plans.
- **Comprehensive Reviews (CRs):** DHS is leading the interagency effort to develop and conduct comprehensive reviews of select potentially high-risk CI/KR. The CR program spans multiple CI/KR sectors. Working collaboratively with the asset owner or operator, local and State law enforcement and first-responders, and other security partners (e.g., FBI, NRC, EPA), a DHS-led interagency team evaluates the potential consequences and vulnerabilities of a given asset or group of like assets from high-consequence and/or high-risk sectors in a geographical area, as well as the protective and response capabilities associated with the asset(s) and the surrounding community. Through the CR process, DHS ensures coordination among security partners, minimizes duplication of CI/KR activities, facilitates the development and improvement of key relationships, identifies and corrects

planning deficiencies, identifies protective measures that can increase regional security, and gathers information to support national comparative risk assessment efforts.

CRs will assist State and local jurisdictions in identifying vulnerabilities and capability gaps so they may be addressed in State and local homeland security strategies and CI/KR protection programs. CRs will offer asset owners and operators benefits such as no-cost reviews of their security posture by CI/KR experts; increased security and response capabilities among local law enforcement and emergency management organizations; validation and recognition of voluntary security efforts undertaken by asset owners and operators and communities; and assistance to ensure compliance with Federal and State regulations related to security. CRs benefit the community by identifying gaps in the response capability with the goal of providing guidance on the allocation and targeting of grant funds to reduce risk. CRs reduce burdens on owners, operators and local officials by consolidating multiple Federal facility visits.

As the CR process matures, DHS expects to learn a great deal about the development and execution of joint programs, and to employ these lessons in building partnerships, thereby increasing the efficiency of Federal CI/KR protection activities, and reinforcing the value of a coordinated approach. Federal agencies with an equity in the security of various sectors should plan and budget for participation in the CR program.

- **Protective Community Support Program:** Specific advisory support is provided to the protective community (e.g., law enforcement, first responders, etc), including training and exercise support.
- **Protective Security Advisor (PSA) Program:** DHS protection specialists are assigned as liaisons between DHS, the protective community and the general public in areas representing major concentrations of CI/KR across the United States. The PSAs are knowledgeable regarding potential targets of value in their assigned areas and are responsible for sharing risk information and providing technical assistance to local law enforcement and the owners and operators of assets within those areas.
- **International Outreach Program:** DHS works with the Department of State to undertake international outreach to foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructures on which the United States depends.
- **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, tribal, local, and international government elements as well as private sector corporations and coordinating councils. The objectives of the National Cyber Exercise Program are to:
    - Sensitize a diverse constituency of private and public sector decisionmakers to a variety of potential cyber threats, including strategic attacks;
    - Familiarize security partners with the cyber response system and the importance of their role in it;
    - Practice effective collaborative response to a variety of cyber attack scenarios, including crisis decisionmaking;
    - Provide an environment for evaluation of interagency and inter-sector business processes reliant on the information infrastructure;
    - Measure the progress of ongoing U.S. efforts to defend against and respond to attacks;
    - Foster improved information sharing among government agencies and between government and private industry; and

  - Practice the roles and responsibilities of government agencies and industry in cyber incident response.

- **Software Assurance:** DHS is developing best practices and new technologies to promote integrity, security, and reliability in software development. DHS is leading the Software Assurance Program, a comprehensive software assurance strategy that addresses people, processes, technology, and acquisition throughout the software development life cycle to result in secure and reliable software that supports mission requirements enabling more resilient organizations. DHS's efforts to achieve a broader ability to routinely develop and deploy trustworthy software products through public-private partnerships will lead to the production of higher quality, more secure software. The Software Assurance Program is designed to lead the development of practical guidance and review tools, and promote R&D investment in cybersecurity.

- **Control System Security Programs:** DHS sponsors programs to increase the security of control systems. A control system is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation's CI/KR (e.g., chemical plants, manufacturing plants, transportation systems, oil and gas refineries, power generation, and transmission systems) and are vulnerable to increasing cyber threats that could have a devastating impact on national security, economic security, public health and safety, and the environment. The DHS Control Systems Security Initiative coordinates efforts among Federal, State, Territorial, tribal and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all CI/KR sectors.

- **Internet Disruption Contingency Planning:** DHS formed a strategic partnership through the Internet Disruption Working Group (IDWG) in January 2005 to coordinate cybersecurity contingency plans, including a plan for recovering Internet functions. This working group collaborates with major security partners to identify and prioritize short-term protective measures necessary to prevent major disruptions of the Internet or reduce their consequences and to identify responsive/reconstitution measures for contingency plans in the event of a major disruption.

- **The National Cyber Response Coordination Group:** The National Cyber Response Coordination Group (NCRCG) facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber Incidents of National Significance and other national cyber incidents and physical attacks that have significant cyber consequences (hereinafter, collectively "cyber incidents"). NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government's response and recovery efforts during a cyber crisis and uses their established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise response and recovery strategies.

- **Federal Cyber System Security Programs:** DHS established the Government Forum of Incident Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation across Federal agencies for cyber system readiness and response efforts. The members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. Other examples of Federal agency cybersecurity access control, certification, and policy enforcement tools include:

  - The General Services Administration (GSA) is responsible for developing and implementing a government-wide infrastructure for authentication services, an automated risk assessment tool for government-wide use in certifying and accrediting its E-Authentication gateway. GSA is creating a list of approved solution providers that supply smart cards based on Federal

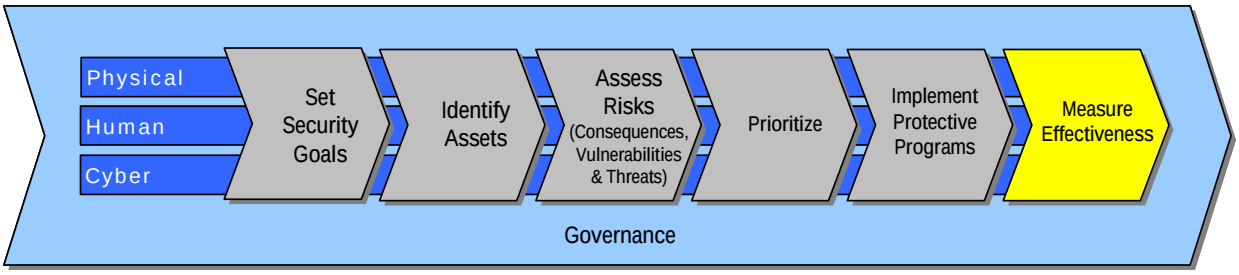
Public Key Infrastructure (PKI) standards and that include a new electronic-authentication policy specification.

- The National Oceanic and Atmospheric Agency (NOAA) has implemented enterprise-wide vulnerability assessments and virus detection software, an intrusion detection system, E500 virus scanning gateways, and a patch management policy.

3.5.3.2 Guidelines, Reports, and Plans

- **Educational Reports:** DHS provides three types of informational reports to support efforts to protect CI/KR. As they are developed, these reports are distributed to all State and Territorial Homeland Security Offices with guidance to share them with owners and operators of CI/KR, the law enforcement community, and captains of the ports in their respective jurisdictions:
  - Characteristics and Common Vulnerabilities (CV) reports identify common characteristics and vulnerabilities at specific CI/KR;
  - Potential Indicators of Terrorist Activity (PI) reports provide information on how to detect terrorist activity in areas surrounding CI/KR; and
  - Protective Measure (PM) reports identify best practices and other protective measures for use in conjunction with specific CI/KR.
- **General Protection Plans:** Generally accepted standards of protection and protective measures for all major classes of assets and special event venues are developed by all CI/KR security partners. They include lessons learned and best practices from national-level vulnerability assessments that are shared with law enforcement officials and industry to allow these parties to enhance the protection of assets that are not nationally critical.
- **Cybersecurity Plans:** Sector-specific cybersecurity plans that are developed to assist SSAs in addressing unique reliance on cyber systems and developing effective and appropriate cyber protective actions.

3.6 Measure Effectiveness



Measuring effectiveness drives continuous improvement of CI/KR protective actions and programs at the sector level and overall program performance at the national level. The NIPP uses a metrics-based system to provide feedback on efforts to attain the goals and objectives articulated in Chapter 1. The metrics also provide a basis for establishing accountability, documenting actual performance, facilitating diagnoses, promoting effective management, and reassessing goals and objectives. Metrics offer a quantitative assessment to affirm that specific objectives are being met or to articulate gaps in the national effort. They also enable identification of corrective actions that may be required and provide decisionmakers with a feedback mechanism to help them make appropriate adjustments. Lessons learned from exercises and actual incidents and alerts provide additional objective input into the process.

3.6.1 NIPP Metrics and Measures

The NIPP includes three types of quantitative indicators to measure program effectiveness:

- **Descriptive Metrics:** Used to understand sector resources and activity; they do not reflect CI/KR protection performance. For instance, a typical descriptive metric would be the number of assets in a given asset class or owner type (e.g., number of chemical manufacturing facilities, percentage of chemical facilities owned by members of the private sector).
- **Process (or Output) Metrics:** Measure whether specific activities were performed as planned, tracking the progression of a task, or reporting on the output of a process such as inventorying assets. Examples of process metrics include the number of vulnerability assessments performed at nuclear power plants by a certain date or the number of chemical facilities that have completed a DHS-approved consequence screen in the previous year. Process metrics show progress toward performing the activities necessary to achieve CI/KR protection goals. They also help build a comprehensive picture of CI/KR protection status and activities.
- **Outcome Metrics:** Track progress toward a strategic goal by beneficial results rather than level of activity. One example of an outcome metric is the change in the number of facilities assessed as high-risk following the implementation of protective actions. Outcome metrics indicate progress toward specific goals or objectives. As the NIPP processes mature, process metrics will be deemphasized in favor of outcome metrics.

Incorporating all three of these quantitative indicators, the specific metrics used in the NIPP will be divided into two groups: (1) core metrics and (2) sector-specific metrics. Core metrics are basic measures that can be tracked across each sector to enable comparison and analysis between different types of CI/KR. Sector-specific metrics are tailored to the unique characteristics of each sector and will be used to assist in monitoring the progress in a specific sector.

3.6.1.1 Core Metrics

Core metrics, common across all sectors, are a set of descriptive, process, and outcome data that enable measurement of progress in SSP implementation. The core metrics are in final development and will be aligned with the key steps in the NIPP risk management framework. Sample core metrics (although not a complete list) are provided in table 3-1.

Table 3-1. Sample Core Metrics

1.	Total number of assets by class.
2.	Number of assets with potential for medium or high consequences.
3.	Percentage of medium- and high-consequence assets with completed vulnerability analyses.
4.	Percentage of medium- and high-consequence assets rated as high-risk.
5.	Percentage of medium- and high-risk assets that have active protective programs to measurably reduce risk.
6.	Percentage of medium- and high-risk assets that have been assessed for readiness, response, and recovery capability.
7.	Percentage of formal security-partner agreements by sector and geographic location.
8.	Percentage of assets reduced from high-risk.

These core metrics will be consistent with the National Preparedness Goal and its supporting Universal Task List (UTL) and Target Capabilities List (TCL). Resources will be allocated to those activities that best accomplish CI/KR protection goals; activities that do advance these goals will be redesigned or eliminated over time.

3.6.1.2 Sector-Specific Metrics

DHS works with the SSAs and security partners to ensure that sector-specific metrics appropriately evaluate program effectiveness and progress within each CI/KR sector. The following are examples of some potential sector-specific metrics:

- Percentage of shipments moving through a specific port that are subjected to detailed screening;
- Number of end users receiving drinking water from a specific Public Water System;
- Amount of energy sector assets using energy assurance technology, tools, or models; and
- Proportion of sole providers of critical pharmaceuticals that have sufficient stockpiles of that pharmaceutical at locations other than the manufacturing facilities.

3.6.2 Gathering Performance Information

DHS works with SSAs to gather the information necessary to measure the level of performance associated with each set of core and sector-specific metrics. Given the inherent differences in CI/KR sectors, a "one size fits all" approach to gathering this information is not appropriate. DHS will work with each SSA to determine the appropriate method that will be included in their SSP. SSAs will identify and, as appropriate, share best practices based on the effective use of metrics to improve program performance.

3.6.3 Assessing Performance and Reporting on Progress

As called for in HSPD-7, a key element to the DHS approach to performance measurement is the annual report that SSAs are required to provide to the DHS Secretary based on an assessment that:

- Determines how sector efforts support the national effort;
- Acts as the overall progress report for each CI/KR sector to track progression against CI/KR protection goals;
- Provides a common vehicle among CI/KR sectors for communicating CI/KR protection performance and progress to security partners;
- Helps to identify best practices from successful programs that can be shared within and among sectors; and
- Provides feedback to DHS and the CI/KR sectors that will be used as input for the continuous improvement of the NIPP.

To prepare this report, DHS will first work with SSAs to assess progress made in each sector and then compile the results into a cross-sector report that describes the progress of CI/KR protection across the Nation. This annual CI/KR report is available for use by senior leadership throughout the government as they allocate the finite resources available for CI/KR activities. The initial sector program assessment conducted is used to establish a baseline against which progress will be measured in future years. A more detailed discussion of the resource allocation process is included in Chapter 7.

In addition to the annual reports, SSAs regularly update CI/KR progress measurements. By maintaining a regularly updated knowledge base, DHS is able to quickly compile real-time CI/KR status reports to respond to tactical intelligence and inform resource allocation decisions throughout the year.

3.7 Using Metrics and Performance for Continuous Improvement

By using NIPP metrics to compare performance to goals, DHS adjusts and adapts the Nation's CI/KR protection approach to account for progress achieved, as well as for changes in the threat and other relevant environments. At the national level, NIPP metrics will be used to focus Federal and security

partner attention on areas of CI/KR that warrant additional resources or other changes. If a comparison of performance and goals using NIPP metrics reveals that there is insufficient progress toward goals (e.g., information-sharing mechanisms have not been established and risk assessments have not been conducted, or one or more sectors have a significant portion of their assets rated as high risk), DHS and its security partners will make policy decisions and undertake actions to focus CI/KR protection efforts on addressing those particular areas of concern.

In addition, the information gathered as part of the risk management framework processes will drive specific CI/KR protection activities. For instance, every time a protective program is implemented, the consequences and vulnerabilities associated with the assets affected by the program change as does its overall risk score and, accordingly, its ranking in the national asset prioritization. Accordingly, the national risk profile is reviewed routinely to ensure that current and prospective allocation of resources are appropriate in light of recently implemented protective measures or other factors such as increased understanding of potential cascading consequences, new threat intelligence, etc.

Not all NIPP-related feedback will be quantitative per se. As part of measuring effectiveness, DHS will work with its security partners to identify lessons learned and best practices. DHS will also work with SSAs to collect all relevant input from their security partners and other sources. DHS and SSAs will ensure that qualitative input is given sufficient weight in assessments of the Nation's ability to meet NIPP goal and supporting objectives.

3.8 Key Implementation Actions

All milestones are specified with respect to the date of final signature of the NIPP. If agencies are not able to meet milestones, they should notify the Secretary of Homeland Security in a letter specifying the reason and the date by which they will be able to achieve the milestone.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
3.1 Set Security Goals								
SSAs SPs	Set sector-specific security goals and objectives that support NIPP goal and objectives.			X				
3.2 Identify Assets								
DHS SSAs	Identify desired asset information by asset type and develop sector asset inventory guidance.			X				
DHS SSAs	Undertake asset identification and data collection efforts.				X			
DHS	Validate submitted information and input the data into the NADB.							Within 180 days of receipt of data
3.3 Assess Risks								
DHS SPs	Develop consequence-based top screen methodology (i.e., RAMCAP Top Screen) for four CI/KR sectors.				X			
DHS SSAs	Initiate performance of consequence-based top screen (i.e., RAMCAP Top Screen) methodology for four CI/KR sectors.					X		

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
DHS SPs	Develop consequence assessment methodology (i.e., RAMCAP Consequence Assessment) for CI/KR sectors with completed top screen methodologies.						X	
DHS SPs	Initiate implementation of consequence assessments (i.e., RAMCAP Consequence Assessment) at CI/KR assets with potentially high consequences (based on results of top screen implementation).							Within 180 days of top screen
DHS SPs	Develop vulnerability assessment methodologies (i.e., RAMCAP SVA modules) for four CI/KR sectors.						X	
DHS SPs	Initiate performance of vulnerability assessment methodologies (i.e., RAMCAP SVA modules) at high-consequence assets in four CI/KR sectors.							Within 90 days of VA method developed
DHS	Perform first quarterly threat assessments on CI/KR sectors.			X				Quarterly
DHS SPs	Develop cross-sector cyber vulnerability assessment best practices.				X			
DHS	Finalize formula to combine the results of normalized consequence, vulnerability, and threat assessments into an asset risk score.						X	
DHS SSAs	Provide guidance, review, and functional cyber expertise to facilitate cross-sector cyber analysis.							X
DHS	Lead the development and conduct of a national cyber threat assessment by leveraging the intelligence community, private-sector security partners, and law enforcement agencies.							X
3.4 Prioritize								
DHS SSAs	Prioritize assets based on normalized risk scores.							As needed to support risk management framework activities
3.5 Implement Protective Programs								
DHS SPs	Identify gaps in protection at the highest risk assets.							Within 180 days of completion of initial asset priority
DHS SPs	Review available protective programs in relation to identified gaps.							Within 90 days of identification of gaps

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
SPs	Begin voluntary implementation of protective programs at the highest risk assets.							Within 90 days of review of available protective programs
DHS SPs	Develop and implement sector-wide protective programs, including dissemination of best practices guidance.							Within 1 year of SSP completion
DHS	Work with IT private sector security partners to develop cross-sector cyber initiatives.							X
3.6 Measure Effectiveness								
DHS SSAs	Develop performance measurement program and associated metrics.	X						
DHS SSAs	Collect data for initial performance measurement effort.						X	
3.7 Using Metrics for Continuous Improvement								
DHS SSAs	Analyze performance measurement data, prepare associated reports and recommendations, and use to refine risk management activities.							Within 90 days of collection of data
KEY: SP = Security Partners, DHS = Department of Homeland Security, SSAs = Sector-Specific Agencies.								

1

4 Organizing and Partnering for CI/KR Protection

The enormity and complexity of the Nation's CI/KR, the distributed character of its protective architecture, and the uncertain nature of the terrorist threat make the effective implementation of protection efforts an enormous challenge. To be effective, the national CI/KR protection strategy must be based on a thorough understanding of these variables and implemented through a coordinated, unified, national approach.

4.1 Leadership and Coordination Mechanisms

The NIPP coordination mechanisms establish linkages between CI/KR protection efforts at the Federal, sector, State, Territorial, tribal, local, regional, and international levels. The structures described below provide a national umbrella that fosters relationships and facilitates coordination within and across protection partners:

- **National-Level Coordination:** The DHS Office of Infrastructure Protection (DHS/OIP) facilitates overall development of the NIPP and SSPs, provides overarching guidance, and monitors the full range of associated coordination activities.
- **Sector Partnership Coordination:** The NIPP Senior Leadership Council, Private Sector Cross-Sector Council, and Sector/Government Coordinating Councils create a structure through which representative groups from all levels of government and the private sector can collaborate and develop consensus approaches to CI/KR protection.
- **State, Territorial, Tribal, and Local Coordination:** The State Administrative Agencies, Homeland Security Advisors, and Emergency Managers coordinate protection-related activities of State, Territorial, tribal, and local planners, administrators, and responders.
- **Regional Coordination:** Regional initiative members and governance bodies, and the Directorate and Steering Committee of the *Homeland Security Regional Initiative* provide CI/KR protection coordination between regions and with DHS and other Federal agencies.
- **International Coordination:** The Interagency Working Group on CI/KR Protection; coordinating bodies for the U.S.-Canada Critical Infrastructure Protection Framework for Cooperation and the U.S.-Mexico Critical Infrastructure Protection Framework for Cooperation; NATO's Senior Civil Emergency Planning Committee; and certain government councils, such as the Council on Foreign Investment in the U.S. provide a range of CI/KR coordination activities associated with established international agreements.

Management of interactions across the groups described above is necessary for several reasons:

- Implementing CI/KR protection within and across various levels of government and the private sector involves overlapping authorities, responsibilities, and resources;
- CI/KR protection planning often involves interaction across various governmental jurisdictions and private sector entities. For example, protection planning for a critical water treatment facility located in a Texas municipality close to the Mexican border would require the SSA to coordinate with the municipal government, State government, regional planning authorities, and international entities with protection responsibilities; and
- Key interdependencies exist between CI/KR, both within and across sectors.

4.1.1 National-Level Coordination

At the national level, DHS oversees and integrates all CI/KR protection activities through the DHS-OIP. In support of security partner coordination, the DHS:

- Leads, integrates, and coordinates the execution of the NIPP, in part by acting as a central clearinghouse for the information sharing and coordination activities of the individual sector governance structures;
- Facilitates the development and ongoing management of these security partner governance/coordination structures/models;
- Ensures that NIPP updates and revisions undergo a comprehensive interagency and public/private review prior to issuance;
- Ensures that consistent policies, approaches, guidelines, and methodologies regarding coordination are developed and disseminated to enable SSAs and other security partners to carry out NIPP responsibilities; and
- Acts as a conduit for the sharing of best practices and lessons learned.

4.1.2 Sector Partnership Coordination

Protecting the Nation's CI/KR requires the development of partnerships between and among government and private sector owners and operators; Federal, State, Territorial, tribal, and local governments; and infrastructure owners and operators, both within and across sectors. The goal of these partnerships is to establish the context, framework, and support for coordination and information-sharing activities required to implement a full spectrum of prudent and responsible protective actions. The Sector Partnership Model encourages formation of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs). The Model also provides guidance, tools, and support so that these groups can work together to carry out their respective protective functions.

Information sharing is both a critical component and a net result of establishing effective partnerships. When owners and operators are provided with a comprehensive picture of threat and participate in ongoing two-way information flow, their ability to assess risks, make prudent security investments, and take protective actions is substantially enhanced. The mechanisms used to share information will vary based on the specific requirements of each sector or group but the overall importance of the partnership framework remains the same. Similarly, when government is equipped with a solid understanding of private sector information needs and requirements, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

The Information Sharing and Analysis Centers (ISACs), established by Presidential Decision Directive 63 (PDD-63) in 1998, provide an important mechanism for information sharing in some of the CI/KR sectors. The ISACs have served as the principal conduits between the public and private sectors for sharing specific threat information (alerts, warnings, and advisories) concerning the Nation's CI/KR. As CI/KR partnerships and coordination continue to evolve towards a fully networked approach to information sharing and decision making (see Section 6.2), a common, robust baseline of communication, and information-sharing capabilities will be needed across and between all security partners. This common baseline will augment the important capabilities and functions of the information-sharing mechanisms, such as ISACs, adapted to the unique requirements of each sector.

ISACs will continue to be a valued security partner under the Sector Partnership Model. The Sector Partnership Model recognizes that not all CI/KR sectors have established ISACs. Additionally, not unlike the sectors they serve, ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical functions). As the sectors define their unique requirements, the ISACs will remain an important information-sharing mechanism for many sectors.

The information-sharing process is designed to communicate both specific threats and information pertaining to the general threat environment (plausible threats, vulnerabilities, potential consequences) so

that owners and operators can assess risks, make security investments, and take protective actions in a rational manner. The Sector Partnership Model provides the framework that enables Government and private sector partners to undertake the full range of protective activities—from risk management to incident response and recovery.

Figure 4-1 illustrates how the Sector Partnership Model is organized. It includes the NIPP Senior Leadership Council (Government), the Government and Private Cross-Sector Councils and a series of Government and Sector Coordinating Councils.

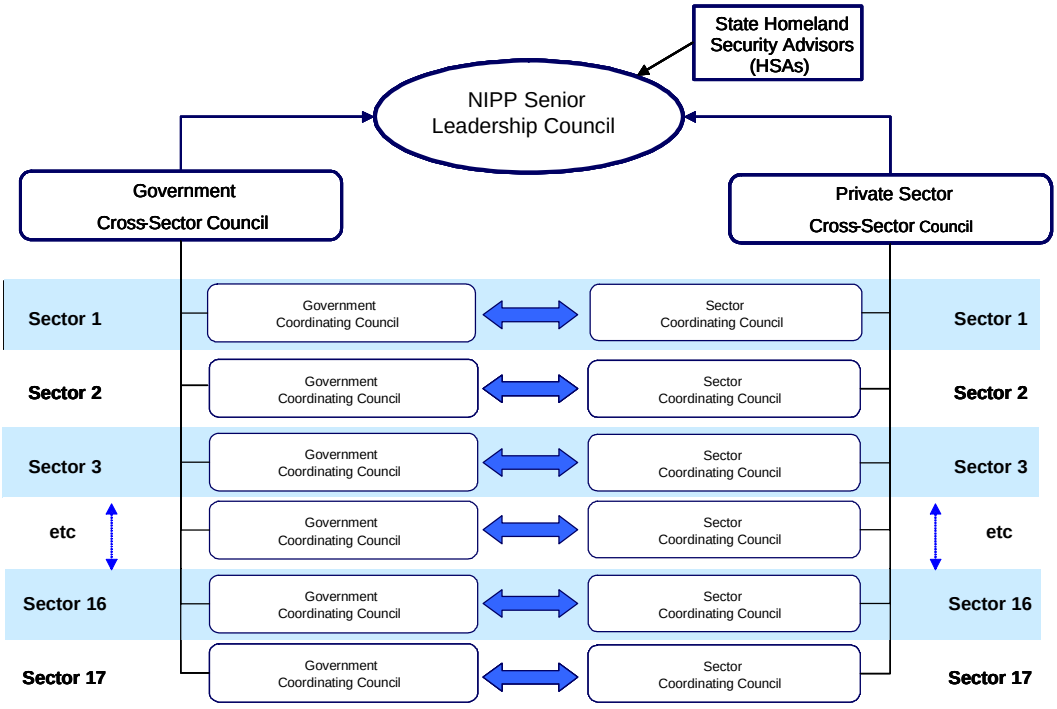


Figure 4-1. Sector Partnership Model

4.1.2.1 Sector Coordinating Councils

The Sector Partnership Model encourages owners and operators to create or identify an SCC as the principal point of entry for developing and coordinating with the Government on a wide range of infrastructure protection activities and issues. SCCs are self-organized, self-run, and self-governed, and are fully representative of a broad base of owners, operators, and associations—both large and small—within a sector.

The SCC charters should contain provisions that ensure inclusiveness and avenues for redress for respective members. SCCs should be broadly representative of the sector, with a spokesperson designated by the sector membership. SCCs are encouraged to constitute themselves in a way that provides for appropriate governance and representation for the sector as a whole. Specific membership will vary sector to sector, reflecting the unique composition of each sector. SCC membership includes various entities such as representative organizations, industry associations, ISACs and/or other appropriate information sharing mechanisms. In some sectors, owner/operators may be governmental organizations, such as municipal water or electric authorities. No single organization—whether an owner/operator or association—should dominate an SCC. Because of the size and diversity of some sectors, the sector may choose to organize into subcouncils to address specific components and their unique issues, with each providing a representative to the SCC. For instance, the Food and Agriculture SCC has formed the

following subcouncils to represent the full "farm-to-fork" spectrum: Producer-Plant, Producer-Animal, Processors-Manufacturers, Restaurants-Food Service, Retail, Warehousing and Logistics, and Agriculture Production Inputs and Services.

The SCCs provide the framework to enable private sector owners and operators to engage DHS and the SSAs. They provide a single point of internal coordination on a wide range of sector-specific infrastructure protection activities and issues. The primary functions of an SCC include:

- Represent a primary point of entry for government into the sector for addressing the entire range of infrastructure protection activities and issues;
- Serve as a focal point for communication and coordination between owners and operators and suppliers, and with the government during response and recovery;
- Identify, implement, and support the information sharing capabilities and mechanisms that are most appropriate for the sector;
- Facilitate inclusive organization and coordination of the sector's policy development, infrastructure protection planning, and plan implementation activities;
- Advise on integration of State, local, and regional planning initiatives with Federal initiatives, such as the State and Local role in sector specific plans, the NIPP and the NRP; and
- Provide input to the government on research and development efforts.

4.1.2.2 Government Coordinating Councils

A GCC is formed as the government counterpart for each sector to enable interagency and cross-jurisdictional coordination. The GCC is comprised of representatives across various levels of government (Federal, State, Territorial, tribal and Local) as appropriate to the security landscape of each individual sector. For example, the Food and Agriculture GCC is comprised of Federal Government agencies including DHS, the Food and Drug Administration, and the U.S. Department of Agriculture; State representatives from the Departments of Agriculture and Health; and local representation from county health departments. In some cases, State and local representation is augmented through the appropriate industry associations (i.e., Association of State and Territorial Health Officials).

The GCC coordinates strategies, activities, policy, and communications across government entities within each individual sector. SCCs and corresponding GCCs work in tandem to create a coordinated national umbrella for infrastructure protection across sectors. The primary functions of a GCC include:

- Provide interagency coordination at the sector operating level through partnership among DHS, the SSA, and other supporting Federal departments and agencies;
- Coordinate strategic communications, issue management, and resolution among government entities within the sector; and
- Coordinate with and support efforts of the SCC to plan, implement, and execute the Nation's CI/KR protection mission.

4.1.3 State, Territorial, Tribal, and Local Government Coordination

State and Territorial Homeland Security Advisors (HSAs) serve as primary jurisdictional points-of-contact for DHS, between governments at all levels, and CI/KR asset owners and operators. State HSAs are a vital component of the Sector Partnership, providing guidance on State-level CI/KR protection strategies and programs. State HSAs provide the knowledge and relationships to augment national CI/KR protection efforts. Other State administrative agencies, designated by the Governor, support development of homeland security strategies, implement strategic goals and objectives, and administer Federal

preparedness assistance. In some cases, State Administrative Agencies (SAAs) also perform the HSA function, while in other cases, these positions are staffed separately. States may use State agencies as sector leads, much as the Federal Government has identified sector-specific agencies in certain cases.

A number of high-threat, high-density communities participating in the Urban Areas Security Initiative (UASI) have established working groups that provide regional, multidisciplinary coordination for developing and implementing homeland security strategies. These UASI working groups also address relevant activities supporting broader regional infrastructure protection activities (if applicable) and the State CI/KR protection program.

4.1.4 Regional Initiative Coordination

Regional initiatives that support CI/KR protection operate across the country to advance the region's (and, collectively, the Nation's) protective posture. They include public-private partnerships that cross jurisdictional, sector, and international boundaries and take into account key dependencies and interdependencies.

Virtually all regional efforts are initiated locally without top-down mandate. Most are specifically motivated by the fact that major homeland security incidents happen in specific locations marked by a high degree of interdependency among infrastructures essential for public health and safety, and economic continuity.

While regional initiatives are managed independently, a coordinating body, the *National Homeland Security Regional Initiative*, has been created to focus on best practices and lessons learned. To maximize coordination of regional initiatives that intersect with international, national, sector, and State and local-based initiatives under the NIPP coordination framework, the Steering Committee for the initiative provides a channel for information-sharing between regional initiatives and DHS, which serve to:

- Ensure compatibility of regional approaches with the NIPP framework;
- Support identification of regional CI/KR, vulnerabilities, interdependencies, and emerging issues;
- Share best practices, accomplishments, and progress; and
- Encourage and enable the establishment of additional regional initiatives and further coordination between public-private partners.

In addition, individual regional initiative managers can maximize intra-regional coordination based on their unique missions by engaging:

- State and Territorial governments through the HSAs to ensure that State CI/KR strategic planning efforts include regional considerations for that State or territory;
- Sector-specific government representatives through the GCCs and private sector representatives through the SCCs to ensure that regional planning efforts are coordinated with relevant sector-specific activities, identify potential regional issues that may require additional sector focus, and share lessons learned and best practices from other regions; and
- International security partners in accordance with international agreements to ensure that regional initiatives include cross-border considerations as appropriate.

The *Pacific NorthWest Economic Region (PNWER)* provides an example of an effective regional initiative. PNWER is a statutory, public-private partnership composed of legislators, governments, and businesses in the Northwest States of Alaska, Idaho, Montana, Oregon and Washington and the Western Canadian Provinces of British Columbia, Alberta, and the Yukon Territory. PNWER established the Partnership for Regional Infrastructure Security in October 2001, and held the first bi-national, multi-jurisdictional CI/KR protection interdependency exercise, Blue Cascades in 2002. This exercise served as

a model for the U.S. Canada Bi-Lateral on CI/KR protection that involved more than 200 participants from five States and two Canadian Provinces. PNWER has since fostered the development of the Puget Sound Regional Partnership that, in cooperation with DHS, held a second Blue Cascades exercise in September 2004 focusing on cyber and physical attacks. A followup Action Plan has been funded through the UASI program and includes 27 current projects such as a cybersecurity council working with the U.S.-Computer Emergency Readiness Team (CERT) on a cyber incident management system for the region and an Interdependency Working group on applying decision and simulation tools to regional CI/KR.

4.1.5 International CI/KR Protection Cooperation

CI/KR assets, both physical and cyber, are inextricably interconnected to the global infrastructures that have evolved to support modern economies. Each of the 17 CI/KR sectors is linked in varying degrees to global energy, transportation, telecommunications, cyber, and other infrastructures. This global system creates tremendous benefits and efficiencies, but also brings unavoidable interdependencies and vulnerabilities. The Nation's prosperity and way of life depend on these "systems of systems," which must be protected both at home and abroad.

The NIPP strategy for international CI/KR protection coordination and cooperation is focused on:

- Instituting effective cooperation with international security partners, rather than on specific protective measures. Specific protection measures are developed through the sector planning process and specified in SSPs;
- Implementing current agreements that affect CI/KR protection; and
- Addressing cross-sector and global issues such as cybersecurity and foreign investment.

International CI/KR protection activities require coordination with the Department of State and must be designed and implemented to benefit the Nation and its international security partners.

4.1.5.1 Cooperation with International Security Partners

DHS will work with the Department of State, international partners, and other entities involved in the international aspects of CI/KR protection, to exchange experiences, share information and develop a cooperative environment to materially improve U.S. CI/KR protection. DHS and SSAs will work with specific countries to identify international interdependencies and vulnerabilities and through international organizations such as the G8, the North Atlantic Treaty Organization (NATO), the European Union, the Organization of American States and the Organisation for Economic Cooperation and Development to enhance CI/KR protection.

While SSAs have primary responsibility for developing protective measures to address risks that arise from international factors, DHS has specific programs to enhance the cooperation and coordination needed to address the unique challenges posed by the international aspects of CI/KR protection:

- **International Outreach Program:** DHS works with the Department of State to conduct international outreach to foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructures on which the United States depends.
- **National Cyber Exercises:** DHS is conducting exercises to identify, test, and improve coordination of the cyber incident response community, to include Federal, State, Territorial, tribal, local, and international government elements, as well as private sector corporations and coordinating councils.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the

"steady-state" protection plans and programs put in place by the NIPP. The exercise program, as appropriate, engages international partners to address cooperation and cross-border issues including those relating to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners.

4.1.5.2 Implementing Current Agreements

Existing agreements with international security partners include bilateral and multi-lateral partnerships. The key partners included in existing agreements include:

- **Canada and Mexico:** The CI/KR relations between the United States and its immediate neighbors make the borders virtually transparent. Electricity, natural gas, oil, roads, rail, food, water, minerals and finished products flow both ways across the borders. The importance of this trade, and the infrastructures that support it, was highlighted after the terrorist attacks of September 11, 2001 nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CI/KR issues. In addition, the 2005 Security and Prosperity Partnership of North America (SPP) established a trilateral approach to common security issues.
- **United Kingdom:** The United Kingdom is a close ally with significant experience in fighting terrorism and protecting its national CI/KR. The U.K. Government has developed an effective, sophisticated system of managing public-private partnerships to help ensure CI/KR protection. DHS has formed a Joint Contact Group with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **G8:** The G8 has underscored its determination to combat all forms of terrorism and to strengthen international cooperation. A number of initiatives launched at recent summits focus on counter terrorism. The G8 heads of government attending the July, 2005 meeting in Glenn Eagles issued a Statement on Counter-Terrorism (http://www.g8.gov.uk). In it they pledged *to "…work to improve the sharing of information on the movement of terrorists across international borders, to assess and address the threat to the transportation infrastructure, and to promote best practices for rail and metro security."*
- **NATO:** NATO addresses CI/KR issues through the Senior Civil Emergency Planning Committee (SCEPC), and has developed considerable expertise that applies to CI/KR protection. DHS has a delegation to SCEPC, participates in the NATO telecommunications working group, and engages with NATO in preparedness exercises.

4.1.5.3 Approach to International Cyber CI/KR Protection

International cooperation in cybersecurity helps to foster national and international activities that promote a global culture of security and improve the Nation's overall incident preparedness and response posture. The United States proactively integrates its intelligence capabilities to protect the country from cyber attack; its diplomatic outreach and advocacy and operational capabilities to build awareness, preparedness, capacity, and partnerships in the global community; and its law enforcement capabilities to combat cyber crime wherever it originates. The effort requires interaction between policy and operational functions to coordinate national and international activity that is mutually supportive across the globe:

- **International Cybersecurity Policy:** The United States is working strategically with key allies on cybersecurity policy and operational cooperation. Leveraging pre-existing relationships among Computer Security Incident Response Teams (CSIRT), DHS has established a preliminary framework for cooperation on cybersecurity policy, watch and warning, and incident response with key allies such as Australia, Canada, New Zealand, and the United Kingdom. The framework also incorporates strategic issue management to address cybersecurity over the long term, including software assurance,

R&D, attribution, control systems, and other factors. When existing CSIRTs are not operational, DHS encourages development of those capabilities through participation in bilateral discussions and programs with countries of interest and with nascent or emerging cybersecurity initiatives.

- **Multilateral Frameworks:** The U.S. Government uses existing multilateral frameworks and newly forming bilateral dialogues to encourage countries to identify key cybersecurity points-of-contact and develop computer security incident response teams. The Asia Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group, for example, has engaged in a capacity-building program to help member countries develop computer emergency response teams. Several countries in the Asia region participate in the Asia Pacific Computer Emergency Response Team (APCERT). The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber crime, the G8 High Tech Crime Working Groups' principles for fighting cyber crime and protecting critical information infrastructure, the OECD guidelines on information and network security, and United Nations General Assembly resolutions based on the G8 and OECD effort.
- **Regional Groups:** DHS, in cooperation with the Department of State, provides leadership in regional forums, such as the Organization of American States (OAS) and APEC, to raise awareness and develop cooperative programs on cybersecurity. The OAS has approved a framework proposal by its Cybersecurity Working Group to create an OAS regional computer incident response network that includes information sharing and capacity building.

4.1.5.4 Foreign Investment in CI/KR

CI/KR protection may be affected by foreign investment and ownership of sector assets. This issue is monitored at the Federal level by the Committee on Foreign Investment in the United States (CFIUS) and, in some cases, the Federal Communications Commission. In February 2003, DHS was added to CFIUS. The council also includes the Secretaries of State, Defense, and Commerce; the Attorney General; the Director of the Office of Management and Budget; the U.S. Trade Representative; and the Chairman of the Council of Economic Advisers, and is chaired by the Secretary of the Treasury.

DHS has important responsibilities on these government commissions that support the NIPP. These responsibilities include assessing the impacts of proposed foreign investments on CI/KR protection, government monitoring activities aimed at ensuring compliance with agreements that result from CFIUS rulings, and supporting executive branch reviews of applications to the Federal Communications Commission from foreign entities to assess if they pose any threat to CI/KR protection.

Appendix H provides additional information on international coordination.

4.2 The Information-Sharing Strategy: A Networked Approach

Efficient information-sharing mechanisms and processes are required to ensure implementation of effective, coordinated, and integrated CI/KR protective measures. However, information sharing is not an end unto itself. Rather, it enables both government and private sector partners to accurately assess events, formulate risk assessments, and determine appropriate courses of action. The NIPP information-sharing network represents a fundamental change in how security partners organize information and make decisions to prepare for, prevent, and respond to threats, incidents, and crises. This change constitutes a shift from a strictly hierarchical to a networked approach allowing movement of information both vertically and horizontally, as well as the ability to enable decentralized decisionmaking. The objectives of the networked approach are to:

- Enable secure multi-directional information sharing between and across government and industry;
- Implement a common set of communication, coordination, and information-sharing capabilities for all security partners;

- Provide asset owners and operators with a robust communications framework tailored to their specific information sharing requirements, risk landscape, and protective architecture;
- Provide a comprehensive threat assessment picture to all security partners, including general and specific threats, incidents and events, impact assessments, and best practices;
- Maximize the ability of security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and sensitivity of shared information.

Figure 4-2 depicts the CI/KR protection-related information-sharing network. In its simplest sense, the NIPP information-sharing network consists of components that are connected by a common Web-based platform so that security partners can obtain, analyze, and share information.

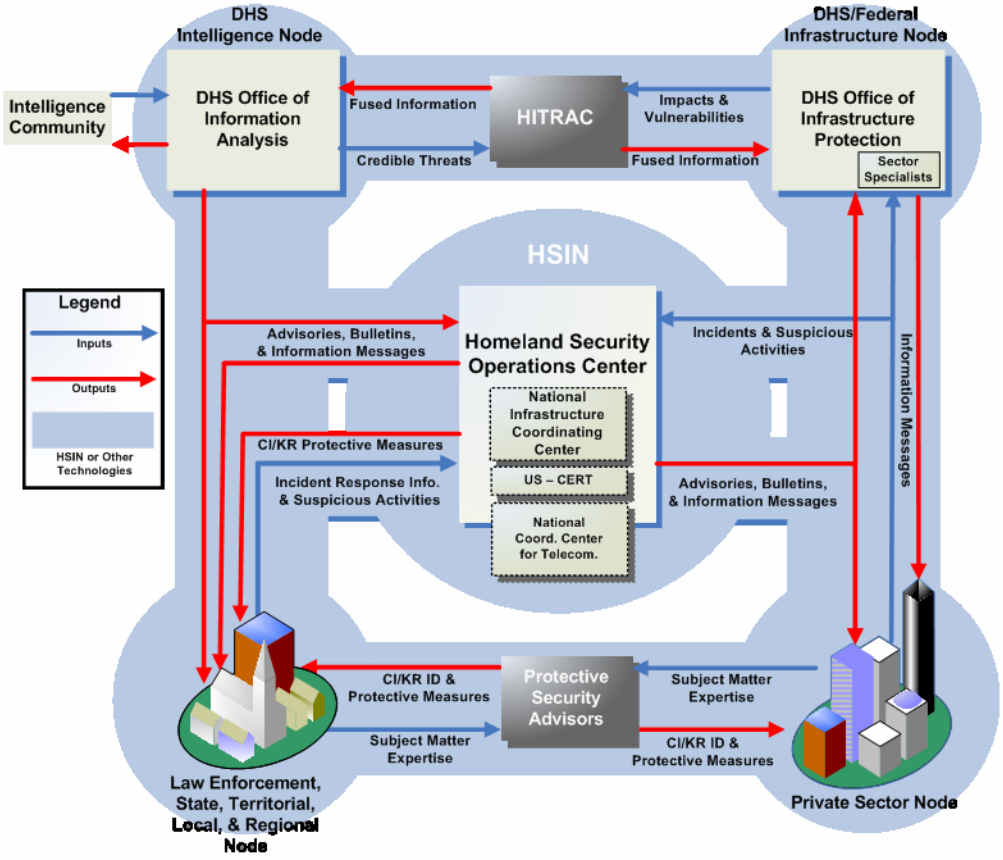


Figure 4-2. NIPP Information-Sharing Network

The NIPP information-sharing network is comprised of the following core components:

- **DHS Office of Information Analysis (DHS/OIA):** DHS/OIA works with the national intelligence community to identify and establish the credibility of general and specific threats. DHS/OIA fuses, assesses, and validates, to the greatest degree possible, information received and generates and disseminates DHS "threat warning products" through the HSOC to security partners.
- **DHS Office of Infrastructure Protection (DHS/IP):** DHS/IP gathers and receives infrastructure incident/event information from a variety of sources, including SSAs, other Federal agencies, and security partners to assess vulnerabilities and the actual or potential impacts of incidents/events.

- **DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC):** HITRAC analysts fuse the credible threat information received from the DHS/OIA with incident/event impact assessments and vulnerability information provided by DHS/IP. Once the information is fused, HITRAC passes its analytical products to both DHS/OIA and DHS/IP to enable situational awareness, additional analysis, or the generation of threat warning products.
- **Law Enforcement and State, Territorial, Regional, Tribal, and Local:** This component provides vital links between DHS and security partners at the State, Territorial, tribal, and local levels. Members provide incident response and first responder information, and report suspicious activities to the FBI and the HSOC for awareness and analysis. HSAs receive and further disseminate DHS threat warning products, as appropriate.
- **Private Sector:** This component includes CI/KR owners and operators, SCCs, ISACs, and trade associations that provide incident, event and suspicious activity reports that may indicate actual or potential terrorist intent. DHS, in return, provides threat warning products, protective strategies, and alert notification to a variety of industry coordination and information-sharing mechanisms, and directly to owners and operators.
- **DHS Protective Security Advisors (PSAs):** PSAs assist efforts to identify, assess, monitor, and minimize risk to CI/KR at the local or regional level. PSAs facilitate, coordinate, and/or perform vulnerability assessments for local CI/KR, and assist with security efforts coordinated by HSAs, as requested.

The linkage of these nodes results in a dynamic view of the total threat and risk landscape. This enhances the effectiveness of each node and, more importantly, the network as a whole. The inputs (identified by blue lines) of one node greatly contribute to and/or initiate the outputs (identified by red lines) of another node. DHS works with security partners to continuously evaluate these components based on current and evolving information requirements thereby providing the ability to measure the efficacy of the network and to identify areas in which new mechanisms or supporting technologies are required.

4.2.1 The Homeland Security Information Network

The Homeland Security Information Network (HSIN) serves as the secure Web-based national communications platform that enables security partners to communicate and share near real-time information with each other and DHS. By offering a user-friendly, efficient conduit for information sharing, the HSIN enhances the combined effectiveness of all security partners in preventing terrorist attacks and preparing for, or responding to, terrorist attacks and natural or manmade disasters.

The HSIN is composed of multiple, non-hierarchal Communities of Interest (COI). This structure allows government and industry partners to engage in collaborative exchanges, based on specific information and security requirements, mission emphasis, or interest level. Table 4-2 provides a brief description of the currently available HSIN COI and "allied" networks and programs that serve, support, or leverage HSIN capabilities and the COI structure.

4.2.2 Watch Operations Centers

The principal purpose of a watch operations center is to collect and share information. Therefore, the value and effectiveness of a watch operations center is largely dependent upon a timely, accurate, and extensive population of information sources. The NIPP information-sharing network integrates several primary watch operations centers to enhance information exchange with security partner operations centers, providing a far-reaching network of awareness and coordination (refer to Figure 4-2).

4.2.2.1 Homeland Security Operations Center

The Homeland Security Operations Center (HSOC) serves as the Nation's hub for information sharing, situational awareness, and domestic incident management, increasing coordination among Federal, State, Territorial, tribal, local, and private sector partners, as well as select members of the international community. As such, it is at the center of the NIPP information-sharing network.

The HSOC houses representatives from more than 35 departments and agencies, including representatives of State and local law enforcement, the Federal intelligence community, and other homeland security and emergency management entities, each supporting and contributing to the vital information-sharing and coordination functions of the center which include:

- **Information Collection and Analysis:** The HSOC monitors vulnerabilities and evaluates them against threats, providing a centralized, real-time flow of information between security partners. An HSOC Common Operational Picture (COP) is generated using data collected from across the country providing a broad view of the Nation's current overall threat status. Using the COP, HSOC personnel perform initial assessments, in coordination with the FBI, to gauge the terrorist nexus and track operational actions taking place across the country in response to the threat. The information compiled by the HSOC is accessible to appropriate security partners via the HSIN.

Table 4-2. HSIN Communities of Interest

COI	Description
Counterterrorism (HSIN-CT)	Enables Federal, State, Territorial, tribal, or local government agencies to share information relating to counterterrorism and incident management.
Critical Sector (HSIN-CS)	Provides a mechanism for information sharing and collaboration within each critical infrastructure sector, across the sectors, and between the sectors and the government.
Emergency Management (HSIN-EM)	Enables information sharing between emergency management personnel at the Federal, State, Territorial, tribal, and local levels, including Emergency Operations Centers (EOCs).
Intelligence	Enables information sharing between authorized users in the intelligence community. Initially being used as a DHS Information Analysis Intranet.
International	Enables information sharing between international partners requiring close coordination with the Homeland Security Operations Center (HSOC).
Law Enforcement (HSIN-LE)	Enables information sharing between all Federal, State, Territorial, tribal, and local departments requiring access to Law Enforcement Sensitive (LES) information. COI members must meet the Department of Justice definition of law enforcement.
Law Enforcement–Analysis (JRIES LE-A)	Enables information sharing between law enforcement departments that have major Intelligence centers and are approved by the Joint Regional Information Exchange System (JRIES) Board.
Secret Network	An interim capability[9] that is used to communicate secret-level information to State Emergency Operations Centers and select police departments.
Other COIs	HSIN provides the capability to develop additional temporary or permanent COIs on an as-needed basis. Examples include HSIN National Special Security Events (NSSE) and HSIN National Capital Region (NCR).
Allied Network	**Description**
Critical Infrastructure (HSIN-CI)	Designed, implemented, and deployed as a regionally coordinated private and public information exchange and alerting forum.

[9] A new DHS backbone, known as the Homeland Secure Data Network (HSDN), is being implemented to securely communicate classified information to all Federal, State, Territorial, tribal, and local agencies capable of receiving secret-level information.

Critical Infrastructure Warning Information Network (CWIN)	A network within HSIN that provides mission-critical, survivable connectivity for DHS, SSAs, HSAs, Emergency Management Centers, and private sector entities vital to restoring the Nation's electric power, information technology, and telecommunications infrastructures.
U.S.-CERT (HSIN-U.S.-CERT)	A focal point for communicating and addressing cybersecurity incidents and other relevant cyber information within the Federal Government.

- **Situational Awareness and Incident Response Coordination:** The HSOC is the primary situational awareness conduit for the White House Situation Room. As such, it provides information needed to make decisions and define courses of action, and serves as primary information-collection and reporting mechanism for the Interagency Incident Management Group (IIMG) as outlined in the NRP.[10]
- **Threat Warning Products:** DHS/OIA develops and disseminated threat warning products to Federal, State, Territorial, tribal, and local governments, as well as to private-sector organizations and international partners through the HSIN. Examples of threat products include:
    - **Advisories:** Contain actionable threat information and provide recommended protective measures based on the nature of the threat. They also may communicate a change, national, regional or sector-specific, in the level of the Homeland Security Advisory System.
    - **Information Bulletins:** Communicate threat information that does not meet the timeliness, specificity, or criticality of advisories but impacts the security of U.S. CI/KR.
    - **Homeland Security Information Messages (HSIMs):** Provide uncorroborated threat information focusing on specific geographical targets, timing or methodology in an expedited manner. A deliberate tradeoff is made to forego the time needed for corroboration and full evaluation by the Intelligence Community in favor of the timeliness of dissemination.

4.2.2.2 National Infrastructure Coordinating Center

The National Infrastructure Coordinating Center (NICC) is a 24/7 watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. As an extension of the HSOC, the NICC provides a centralized mechanism and process for information sharing and coordination between and among government, SCCs, GCCs, and other industry partners.

The NICC receives situational, operational, and incident information from CI/KR sectors, in accordance with information-sharing protocols established in the NRP. The NICC also disseminates a wide range of products containing warning, threat, and CI/KR protection information to security partners. Examples of NICC information exchange include the following:

- **Alerts and Warnings:** The NICC disseminates threat-related information products to an extensive customer base of industry partners.
- **Suspicious Activity and Potential Threat Reporting:** The NICC receives and processes reports from the private sector on suspicious activity or potential threats to the Nation's CI/KR. The NICC documents the information provided, compiles additional details surrounding the suspicious activity or potential threat, and disseminates the report to DHS Sector Specialists, HSOC, and the FBI.

[10] The IIMG is a headquarters-level group comprised of senior representatives from DHS components, other Federal Departments and agencies, and nongovernmental organizations. The IIMG provides strategic situational awareness, synthesizes key intelligence and operational information, frames operational courses of action and policy recommendations, anticipates evolving requirements, and provides decision support to the Secretary of Homeland Security and other National authorities during periods of elevated alert and National domestic incidents.

- **Incidents and Events:** When an incident or event occurs, the NICC coordinates with DHS Sector Specialists, industry partners, and other established information-sharing mechanisms to communicate pertinent information. As needed, the NICC generates reports detailing the incident as well as the impacted (or potentially) impacted sectors and disseminate them to the HSOC.
- **National Response Planning and Execution:** The NICC supports the NRP by facilitating information sharing among SCCs, GCCs, ISACs, and other security partners during mitigation, response, and recovery activities.

4.2.2.3 National Coordinating Center for Telecommunications

The National Coordinating Center for Telecommunications (NCC) is a joint industry-government entity that regularly passes situational and operational information to the HSOC and other DHS components. The NCC coordinates with industry and Federal Government organizations involved in National Security/Emergency Preparedness (NS/EP) telecommunications service requirements.

In support of the NIPP, the NCC serves as the mechanism by which the Federal Government and the telecommunications industry jointly respond to NS/EP telecommunications service requirements. The NCC provides the capability to rapidly exchange information and expedite NS/EP telecommunications response. While the primary focus of the NCC is the NS/EP telecommunication service requirements of the Federal Government, the NCC also monitors the status of all essential telecommunication facilities, including public switched networks.

4.2.2.4 U.S.-Computer Emergency Readiness Team

The U.S. Computer Emergency Readiness Team (U.S.-CERT) is a 24/7 single point of contact for cyberspace analysis warning, information sharing, and incident response and recovery for security partners. It is a partnership between DHS and the public and private sectors designed to enable protection of the Nation's Internet infrastructure and to coordinate the prevention of, and response to, cyber attacks across the Nation.

U.S.-CERT coordinates with security partners to disseminate reasoned and actionable cybersecurity information through a Web site, accessible via the HSIN, and through mailing lists. Among the products it provides are:

- **Cybersecurity Bulletins:** Weekly bulletins written for systems administrators and other technical users that summarize published information concerning new security issues and vulnerabilities. They are published weekly and are written primarily for system administrators and other technical users.
- **Technical Cybersecurity Alerts:** Written for system administrators and experienced users, technical alerts provide timely information about current security issues, vulnerabilities, and exploits.
- **Cybersecurity Alerts:** Written in language for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.
- **Cybersecurity Tips:** Tips provide information and advice on a variety of common security topics. They are published biweekly and are written primarily intended for home, corporate, and new users.
- **National Web Cast Initiative:** DHS, through U.S.-CERT, and the Multi-State Information-Sharing and Analysis Center (MS-ISAC) has launched a joint partnership to develop a series of national Web casts that will examine critical and timely cybersecurity issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.

U.S.-CERT also provides a method for citizens, businesses, and other important institutions to communicate and coordinate directly with the U.S. Government on matters of cybersecurity. The private

sector can use the protections afforded by the Critical Infrastructure Information Act to electronically submit proprietary data to U.S.-CERT.

4.2.3 Other CI/KR Information-Sharing Components and Technologies

DHS and security partners have established other important information-sharing components and technologies that serve unique functions and enhance information sharing.

4.2.3.1 Other Private Sector Information-Sharing Mechanisms

Accurate and timely information sharing enables owners and operators to effectively manage risk, resulting in a coordinated series of investments, protective strategies, partnerships, and mitigation plans to protect CI/KR. The NIPP network connects and augments existing information-sharing mechanisms, where appropriate, to reach the widest possible population of infrastructure owners and operators. Owners and operators have the greatest understanding of their own physical and cyber assets and systems, and can best determine which security measures and investments will be most appropriate for addressing the risks. Two examples include:

- **Information Sharing and Analysis Centers (ISACs):** ISACs are sector-specific entities that advance physical and cyber CI/KR protection efforts by establishing and maintaining frameworks for interaction between and among members and external security partners. ISAC functions include, but are not limited to: supporting the sector's specific information/intelligence requirements for incidents, threats and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical or other threats; establishing and maintaining dialogue with appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness. ISACs vary in size, scope and complexity providing an array of options that may be used to support the unique information-sharing requirements as defined for each sector by the SCCs. These options include a variety of capabilities such as: watch centers with regular business hours or 24/7 operations; call centers to enable members to contact analysts via telephone or pager during periods of increased activity; and/or Web sites that allow members to access sector-related alerts, warnings, and incident information. ISACs offer important mechanisms capable of disseminating DHS-issued threat information and facilitating real-time security collaboration across sector partners.

- **Other Private Sector Information-Sharing Mechanisms:** Each sector has the ability to implement a tailored information-sharing solution that may include ISACs or other new and/or existing mechanisms, such as trade associations, security organizations, and industry-wide or corporate operations centers, working in concert to expand the flow of knowledge exchange to all infrastructure owners and operators.

4.2.3.2 Use of Supporting Technologies

DHS, other Federal agencies, and the law enforcement community use supporting technologies that provide information to a broad range of security partners. These outreach activities include:

- **Cybercop Portal:** The DHS-sponsored Cybercop Portal is a secure Internet-based information-sharing mechanism that connects more than 5,300 members of the law enforcement community worldwide (including investigators banks and the network security community) involved in electronic crimes investigations.

- **Web-Based Services for Citizens:** A variety of Web-based information services are available to enhance the general awareness and preparedness of American citizens. These include CitizenCorps.gov, FirstGov.gov, Ready.gov, and USAonwatch.org.

- **Sharing National Security Information:** The ability to share relevant classified information poses a number of challenges particularly when the majority of industry facilities are neither designed for, nor accredited to receive, store, and dispose of these materials. HSIN may be used to more efficiently share appropriate classified national security information with private sector owners and operators during incidents, times of heightened threat, or on an as-needed basis. However, until supporting technologies and policies are identified to satisfy this requirement, DHS will continue to expand its initiative to sponsor security clearances for designated private sector owners and operators.
- **Interagency Cybersecurity Efforts:** Interagency cooperation and information sharing are essential to improving national counterintelligence and law enforcement capabilities pertaining to cybersecurity. The intelligence and law enforcement communities have various official and unofficial information-sharing mechanisms in place. Examples include:
    - **U.S. Secret Service's Electronic Crime Task Forces (ECTFs):** ECTFs provide interagency coordination on cyber-based attacks and intrusions. At present, 15 ECTFs are in operation, with an expansion planned in the near future.
    - **FBI's Inter-Agency Coordination Cell (IACC):** The IACC is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
    - **DOJ's Computer Crime and Intellectual Property Section (CCIPS):** The FBI and the Secret Service meet regularly to coordinate and deconflict investigations, ensuring there is no duplication of effort.

4.3 Protection of Sensitive Critical Infrastructure Information

The increased volume of CI/KR-related information sharing among government and private sector partners raises a significant concern regarding the protection of sensitive information. DHS has, therefore, instituted a number of programs and procedures to ensure that critical infrastructure information is properly safeguarded.

4.3.1 Critical Infrastructure Information Act

The Protected Critical Infrastructure Information (PCII) Program was established pursuant to the Critical Infrastructure Information (CII) Act of 2002. The Act creates a new framework that enables members of the private sector to voluntarily submit sensitive information regarding the Nation's infrastructure to DHS with the assurance that the information will be protected from public disclosure. The Act allows the department to share this information with other government entities that have homeland security responsibilities.

4.3.1.1 PCII Program Office

DHS established the PCII Program Office to manage information, develop protocols for how to care for "voluntarily submitted critical infrastructure information," and raise awareness regarding the removal of impediments to information sharing regarding cyber and infrastructure vulnerabilities between the public and private sectors.

The PCII Program Office is responsible for receiving, validating, and safeguarding critical infrastructure information submitted to DHS. The Program Office will work with government programs to facilitate information sharing with the private sector. The Program Office establishes partnerships with government users of critical infrastructure information and those entities in the private sector willing to share their information on a voluntary basis. Government entities seeking to access PCII must meet safeguarding requirements as defined by the Program Office.

4.3.1.2 Critical Infrastructure Information Protection

The following general process applies for CII submissions:

- The PCII Program Office will first validate that the information qualifies for protection under the Act;
- All validated PCII will be stored in a secure data management system. All original PCII remains in the data management system and only copies are shared with authorized users. Secure methods will be used for disseminating PCII;
- Authorized users must comply with safeguarding requirements defined by the PCII Program Office; and
- Any suspected disclosure of PCII will be promptly investigated. Federal employees may face significant fines or penalties for improper disclosure.

4.3.1.3 Potential Uses of PCII

PCII may be shared with authorized government entities for purposes of securing critical infrastructure and protected systems. PCII will be used for analysis, prevention, response, recovery, or reconstitution of CI/KR threatened by terrorism or other hazards:

- Authorized government entities may generate advisories, alerts, and warnings relevant to the private sector based on the information provided. Any communications made available to the public must not contain any sensitive information provided by the submitter; and
- PCII can be combined with other information, including classified information, to construct actionable knowledge. All PCII used in such products must be marked accordingly.

4.3.2 Physical and Information Security

DHS has instituted strict physical and information security protocols to protect sensitive critical infrastructure information collected, processed, stored, and disseminated as part of the NIPP. Physical security protocols require approved access controls and risk mitigation measures for DHS facilities[11]. Information security protocols include access controls, login restrictions, session tracking, and data labeling.

4.4 Privacy and Constitutional Freedoms

Mechanisms detailed in the NIPP are designed to provide a balance between achieving a high level of security and protecting the civil rights and liberties that form an integral part of the national character of the United States. Achieving this balance requires acceptance of some level of terrorist risk. In providing for effective protection measures, the processes outlined in the NIPP respect privacy, the freedom of expression, the freedom of movement, the freedom from unlawful discrimination, and other liberties that define the American way of life.

Compliance with the Privacy Act and governmental privacy regulations and procedures are a key factor considered when collecting, maintaining, using, and disseminating personal information. The following DHS offices support the NIPP processes:

- **DHS Privacy Office:** DHS has designated a Privacy Officer to ensure that it appropriately balances mission with civil liberty and privacy concerns. The officer consults regularly with privacy advocates, industry experts, and the public at large to ensure broad input and consideration of privacy issues so that DHS achieves solutions that protect privacy while enhancing security; and

[11] The architecture for the primary system containing sensitive critical infrastructure information must be located in a secure facility that has been accredited for use by the DHS Chief Information Officer or equivalent.

- **DHS Office for Civil Rights and Civil Liberties:** Established to review and assess allegations of abuse of civil rights or civil liberties, racial or ethnic profiling, and to provide advice all DHS components.

4.5 Key Implementation Actions

All milestones are specified with respect to the date of final signature of the NIPP. If agencies are not able to meet milestones, they should notify the Secretary of Homeland security in a letter specifying the reason and the date by which they will be able to achieve the milestone.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
4.1 Leadership and Coordination Mechanisms								
DHS	Commence SSC and GCC operations using the NIPP Sector Partnership Model.	X						
DHS	Establish a point within the department for national-level NIPP security partner coordination.	X						
DHS	Establish a dialogue with the Steering Committee of the cross-regional coordinating body to examine options for encouraging regional initiatives, exchange of best practices, emerging issues, accomplishments, and progress, at the national level.			X				
State Tribal Local	Recommend reviewing established coordination mechanisms to ensure they can accommodate the requirements of the NIPP, SCCs and GCCs.				X			
4.2 Information-Sharing Mechanisms								
DHS	Complete rollout of HSIN-CS to all sectors within the NIPP Sector Partnership Model.						X	
DHS	Implement information-sharing processes described in the NIPP.							X
DHS	Implement policies and protocols for vetting and disseminating routine information products to owners and operators, based on the needs of the sectors.	X						
4.3 Protection of Sensitive Critical Infrastructure Information								
DHS	Complete and publish the PCII Final Rule.			X				
4.4 Privacy and Constitutional Freedoms								
	No actions under this category.							
KEY: SP = Security Partners, DHS = Department of Homeland Security, SSAs = Sector-Specific Agencies.								

5 Integration with Other Plans

This chapter describes the relationships between all plans that support the overall national preparedness mission—to prevent, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. The primary focus of this chapter is to describe the linkages between the NIPP and other plans that support preparedness across all levels of government and between the public and the private sectors.

Planning and support of the NIPP is underpinned by a host of activities and practices well established in government and industry. It is common and in some cases required for asset owners and operators to conduct vulnerability assessments and risk assessments, assess their facilities for security and safety hazards, and develop protective action and emergency response plans to mitigate risk. At most levels of government and industry, continuity of operations plans, emergency preparedness plans, CI/KR protection plans, and emergency response plans currently exist and are well documented and implemented.

5.1 Sector-Specific Plans

Each SSA will work with their security partners to develop, implement, and update an SSP, based on NIPP guidance on structure and content, so that protective programs, public and private protection investments, and resources are focused effectively and efficiently within and across sectors. Although SSPs are developed as stand alone documents, they are linked to the NIPP and provide a means by which the NIPP framework is implemented within and across sectors to reduce overall national risk. SSPs also provide a national-level framework for each individual sector that informs the development, implementation and update of State and local homeland security strategies and CI/KR protection programs.

Figure 5-1. Sector-Specific Plan

The SSPs serve the following purposes:

- Define sector security partners, authorities, and interdependencies;
- Establish procedures for sector interaction, information sharing, coordination, and partnership;
- Establish sector-specific goals and objectives to achieve the desired end state protective posture; and
- Identify the approach or methodology by which SSAs conduct the following activities:
    - Identify priority CI/KR within the sector;
    - Assess risks to terrorist attack to include potential consequences of vulnerabilities, and threats;
    - Prioritize assets within a sector as a starting point for determining where protective actions are needed most;
    - Develop protective programs based on the detailed knowledge of sector operations;
    - Inform the development of State and local jurisdiction homeland security strategies and plans; and

- Use metrics to measure and communicate program effectiveness and risk reduction within the sector.

The structure for SSPs (as shown in figure 5-1) facilitates cross-sector comparisons and coordination. Appendix E provides a more detailed discussion of the content required for each chapter of the SSPs.

SSPs are based on a security vision for each CI/KR sector. Each sector vision articulates the sector's desired end state for its CI/KR protection posture. Each vision is tailored to the unique circumstances, resources, and challenges of the sector. The sector specific security visions for the Nation's CI/KR sectors have been developed by the sectors and are presented in Appendix F.

5.2 The National Response Plan

The NIPP and the NRP together provide a comprehensive, integrated approach to addressing key elements of the Nation's homeland security mission to prevent terrorist attacks, reduce vulnerabilities and respond to incidents in an "all-hazards" context. The NIPP determines the ongoing "steady-state" programs to improve the Nation's CI/KR protective posture, while the NRP provides the overarching framework, mechanisms and protocols required for effective and efficient domestic incident management.

The Homeland Security Advisory System (HSAS) provides a progressive and systematic approach to match protective measures to the Nation's overall threat environment. This link between the current threat environment and the required levels of protection provides the means to transition from the "steady-state" processes detailed in the NIPP to the incident management processes described in the NRP. DHS and security partners develop and implement protective measures appropriate for the threat levels specified by the HSAS. As the threat levels increase and the NRP is implemented, DHS and security partners use NRP mechanisms to facilitate those CI/KR protection actions directly related to the current threat status.

5.3 Other Preparedness Plans

Security partners should review and revise as necessary, all preparedness plans to ensure that they are consistent with the NIPP. Examples of plans that may contain prevention, protection, response, and recovery activities that relate to or affect CI/KR protection include:

Infrastructure & buffer zone protection plans	*Emergency preparedness plans*
Continuity of operations plans	*Integrated contingency plans*
Continuity of government plans	*Environmental, health, and safety plans*
Operational and Emergency Response Plans	*Incident Action Plans*

The following sections discuss specific plans that Federal, State, Territorial, and regional authorities should review and coordinate with the NIPP.

5.3.1 Federal Contingency Plans

Contingency planning is a key element of CI/KR protection. Federal security partners will review and revise contingency plans to ensure that there is a seamless link between the NIPP "steady-state" programs and incident-related activities addressed in their contingency plans. Examples of these plans include:

- Continuity plans required by the Federal Information Security Management Act and monitored by OMB;
- OMB-mandated plans for protection of Federally owned or operated CI/KR required by HSPD-7 paragraph 34; and

- Federal Executive Branch Continuity of Operations Plans (COOP) required by Presidential mandate to ensure the ability of Federal departments and agencies to continue to perform their essential functions under a broad range of emergency circumstances.

5.3.2 State and Territorial CI/KR Protection

The NIPP framework is coordinated with State CI/KR protection planning through the DHS Office for State and Local Government Coordination and Preparedness (OSLGCP). To receive Federal grant funds, States must develop a strategy for preparedness based on DHS guidance and submit it to DHS for review and determination of levels of funding. Starting with the fiscal year (FY) 2006 grant application guidance, CI/KR protection will be considered as one of the criteria for evaluating the strategies to determine levels of funding. This provides an important mechanism for HSAs to develop and implement State and Territorial CI/KR protection plans based on the NIPP.

5.3.3 Regional CI/KR Protection

Using the NIPP for regional planning efforts provides a common basis for security partners across boundaries and other jurisdictional lines. The NIPP framework, for example, is being applied in the National Capital Region (NCR)[12] through the development of a regional framework that will build on existing regional preparedness capabilities and augment private, local, State, Territorial, and Federal security and emergency management plans and programs. It will include interdependency exercises to bring the public and private sectors together around shared understanding of the challenges to regional resilience in the NCR, analytical tools to inform decisionmakers on risk and risk reduction with associated benefits and costs, and forums to enable decisionmakers to decide on common solutions to problems and funding within and across sectors and jurisdictions. Using the NIPP framework across a region in this way can benefit CI/KR protection planning efforts across the country.

5.4 Key Implementation Actions

All milestones are specified with respect to the date of final signature of the NIPP. If agencies are not able to meet milestones, they should notify the Secretary of Homeland Security in a letter specifying the reason and the date by which they will be able to achieve the milestone.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
5.1 Sector-Specific Plans								
SSAs	Review NIPP Base Plan requirements and establish program management structures and processes necessary to support implementation of the NIPP within their sector.		X					
SSAs	Complete the development of an SSP for their sector.				X			
DHS	Coordinate with SSAs to ensure that SSPs are completed and meet the national requirements established in the NIPP.				X			

[12] ***NCR*** encompasses a high concentration of closely located Federal, State, and local government entities with overlapping jurisdictions including the District of Columbia; Montgomery and Prince George's Counties in Maryland; Arlington, Fairfax, Loudon, and Prince William Counties and the City of Alexandria in Virginia; and all cities and other units of government within those jurisdictions.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
DHS	Review SSPs to determine if cross-sector coordination requirements are identified.					X		
SSAs	Plan and implement outreach and engagement activities to obtain an adequate cross-section of security partner participation.							X
SSAs	Coordinate with DHS to ensure that revised SSPs respond to and meet the requirements established in the NIPP.							X
5.2 The National Response Plan								
DHS SPs	Review current CI/KR protective measures to ensure they are aligned to the threat levels of the HSAS: • Federal agencies: Action required. • State, Territorial, tribal, and local governments: Action recommended. • Private sector: Action encouraged.		X					
DHS SPs	Revise and implement CI/KR protective measures as required to ensure alignment with the HSAS: • Federal agencies: Action required. • State, Territorial, tribal, and local governments: Action recommended. • Private sector: Action encouraged.				X			
5.3 Other Preparedness Plans								
SPs	Review and modify contingency plans at the national (including sector), State, Territorial, tribal, and local levels to ensure that there is a seamless linkage between the NIPP "steady-state" CI/KR protection programs and other preparedness-related activities: • Federal agencies: Action required. • State, Territorial, tribal, and local governments: Action recommended. • Private sector: Action encouraged.						X	
KEY: SP = Security Partners, DHS = Department of Homeland Security, SSAs = Sector-Specific Agencies.								

6 Ensuring an Effective, Efficient Program Over the Long Term

The effort to ensure an effective, efficient CI/KR protection program over the long term includes the following components:

- **National Awareness** to support the sustainability of the CI/KR protection program, security investments, and protection activities by ensuring a broad understanding by the public, business, and communities of the terrorist threat environment and of what is being done to protect the Nation's CI/KR against such threats;
- **Education and training** to ensure skilled and knowledgeable professionals are able to undertake NIPP-related responsibilities in the future;
- **Research and development** to improve protective capabilities or to dramatically lower the costs of existing capabilities so that sector security partners can afford to do more with limited budgets;
- **Building and maintaining** the currency of databases and data systems to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management; and
- **Continuously improving** the NIPP and associated plans and programs through ongoing management and maintenance activities.

6.1 Building a Program for National Awareness

The development and implementation of a national awareness program for CI/KR protection was identified as a major need by the President's CI/KR protection strategy. DHS, in conjunction with SSAs and other security partners, is responsible for developing and implementing a comprehensive national awareness program that supports the sustainability of the CI/KR protection program, security investments, protection activities, and the public understanding of the terrorist threat environment.

Objectives of the national awareness program are to:

- Create national awareness of the need to incorporate security consideration into business planning and operations to include employee education and training programs across all levels of government and the private sector;
- Support public and private sector decisionmaking and enable the planning of relevant and effective protection strategies and resource allocation;
- Maintain public understanding of the evolving threat to CI/KR as assessed by the Intelligence Community and in the context of the HSAS; and
- Foster public confidence in CI/KR protection efforts to address the threat environment.

DHS also is engaged in a comprehensive national cyberspace security awareness campaign to remove impediments to sharing vulnerability information between security partners. The campaign includes audience-specific awareness materials, expansion of the Stay Safe Online campaign, and development of awards programs for those in industry who make significant contributions to the effort.

6.2 Education and Training

Ensuring a coherent program over the long term requires investment in human capital through education and training. It also requires the organizational and sector expertise that comes from exercises and other forms of practice, testing, and learning. The NIPP highlights the broad set of skills needed to enhance protection of the Nation's CI/KR. Some of these skills, such as the NIPP risk analysis and management framework, are unique cutting-edge approaches that are not yet widely practiced. As such, a cadre of

educated and trained CI/KR protection and risk management professionals is essential to effective implementation of the NIPP and supporting SSPs over the long term.

6.2.1 Build and Maintain Human Capital

CI/KR protection professionals must be educated in the academic, professional, and technical skill sets on which the NIPP and SSPs are based. This requires a training effort with a national scope that includes:

- Technical training to provide workers and technicians with the skills needed to perform their roles and responsibilities under the NIPP;
- Professional education incorporating the latest advances in CI/KR protective approaches, and where appropriate, certification based on government, industry, and professional society standards; and
- Academic and research programs that result in formal degrees from accredited institutions.

Some CI/KR protection workers may require new and highly specialized skills while others rely on established disciplines that are similar to those that enable implementation of effective incident response, emergency management, and personnel surety programs. To ensure workers with the correct skill sets are available to implement the NIPP, DHS will focus its human capital building efforts on those specialized disciplines that are unique to CI/KR protection and leverage accredited academic, professional certification standards, and extensive technical training programs that are in place for the more mature and established disciplines.

6.2.2 Build and Maintain Organizational and Sector Expertise with Exercises

Building and maintaining organizational and sector expertise requires comprehensive exercises conducted to test the interaction between the NIPP and the NRP in terrorist incidents, natural disasters and other emergencies. DHS and SSAs must work together to ensure that these exercises include adequate testing of "steady-state" CI/KR protection measures and plans, including the ability for a protected core of life-critical infrastructure services such as power, food and water, and emergency transportation to withstand attacks or natural disasters and continue to function.

6.2.3 Unique and Critical Expertise Requiring Special Emphasis

DHS generally will focus its stewardship efforts on those skills that are unique to or critical for CI/KR protection and, therefore, warrant special emphasis. These are:

- Cybersecurity;
- Risk management and analysis techniques;
- Cost-benefit analysis based on risk management;
- Insider threat related to infrastructure security;
- Infrastructure dependency and interdependency analysis; and
- Best practices for CI/KR protection.

6.2.4 DHS Role and Approach

Given the scope and nature of the education and training needs related to CI/KR protection, the DHS role will be to encourage and, where appropriate, facilitate specialized NIPP training, professional training, continuing education, and development of professional and personnel surety standards; encourage academic and research programs; and coordinate with exercise managers on the design of exercises that test the interaction between the NIPP framework and the NRP. DHS will also provide for the initial training on the NIPP that is necessary to develop the instructional materials and the core of instructors needed to introduce all security partners to the Plan's contents and requirements.

6.2.4.1 Specialized NIPP Training

NIPP training topics for managers and staff responsible for CI/KR who require special emphasis include:

- Intent, content, and relationship of relevant national strategies, directives, and plans;
- Security partner composition, coordination mechanisms, roles, and responsibilities;
- Special considerations for CI/KR protection:
    - Sector-specific nature of CI/KR protection;
    - Partnerships and coordination;
    - The cyber dimension;
    - The human element; and
    - International CI/KR protection;
- Risk Management Framework, to include risk analysis, assessment, and management as well as the dynamic nature of the terrorist threat;
- CI/KR and cyber asset identification and prioritization;
- CI/KR asset dependencies and interdependencies;
- Programs, initiatives, and support available to security partners;
- Information, privacy, and civil liberty protection;
- Measuring effectiveness and performance of programs and reporting;
- Using sector-specific and core metrics for cost-benefit analysis to improve performance of programs;
- Risk management analysis tools, including data systems, modeling, simulation, and associated analytics;
- Information-sharing mechanisms, coordinating networks, and flow;
- Relationship to, and coordination with, other national planning efforts;
- Input to long-term NIPP components such as:
    - National CI/KR awareness;
    - Education and training programs;
    - R&D planning;
    - NIPP and SSP update; and
    - Database, simulation and analytic tool development process;
- Management of the CI/KR protection program including the interagency decision process for resource allocation; and
- Grant programs available to security partners for targeted CI/KR protection improvements.

DHS will provide or coordinate the development of course materials on these topics and work with security partners to facilitate the definition of general training requirements, and guide the development of national-level training standards associated with the NIPP. DHS will facilitate initial training in these topics for security partners as appropriate.

6.2.4.2 Technical CI/KR Protection Training

DHS supports technical CI/KR protection training programs for security partners to enhance the knowledge and skills required to detect, deter, and defend against terrorist activities that threaten CI/KR. Training resources are provided to local law enforcement and others, with a special focus on urban areas with significant clusters of CI/KR, localities where high profile special events are scheduled, or other potentially high-risk geographic areas. Some of the courses offered by DHS include:

- **Critical Infrastructure Protection Training Program:** A four-and-a-half-day program designed for the Security Manager or Senior Security Specialist. The program addresses protection of those physical- and cyber-based systems essential to the operation of the economy and government, including telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private.
- **Buffer Zone Protection Plan Workshop:** A one-day workshop designed to teach public officials how to perform vulnerability assessments of the areas surrounding a facility from which terrorists may conduct surveillance or launch an attack (the "Buffer Zone"). Completion of this workshop provides local law enforcement with the requisite knowledge to complete a Buffer Zone Protection Plan (described in Chapter 3).
- **Workforce Terrorism Awareness/Prevention Course:** Web-based, two-and-a-half-hour program with knowledge checks designed to enhance work force vigilance by providing instruction on deterrence, detection, and reporting procedures. Participants receive an Online DHS Certificate of Training upon successful completion.
- **Surveillance Detection Course:** A three-day course designed to give municipal and State officials and security managers training on terrorist surveillance tactics and techniques, available detection measures, and ways to identify terrorist activities and surveillance.
- **High Risk Target Awareness Course:** A four-hour information-sharing and learning sessions provide baseline prevention and awareness training to first-level supervisors and security personnel at malls/shopping centers, places of worship, stadiums, educational facilities, arenas, hotels, and large buildings. The primary objective of these sessions is to increase vigilance to deter, detect, and report surveillance, suspect activity, and suspect items.
- **WMD Incident Training for State and Local First Responders:** A program of tailored training to enhance the capacity of State and local jurisdictions to prevent, deter, and respond safely and effectively to incidents of terrorism involving weapons of mass destruction (WMD).
- **Cybersecurity Awareness and Training:** DHS is involved in establishing and influencing cybersecurity training, education, and awareness programs through:
    - Promoting more secure "out of the box" installation and use of cyber products, including increasing user awareness of the security features in products; ease of use for security functions; and, where feasible, promotion of industry guides;
    - Implementing and encouraging the establishment of programs to leverage the existing Cyber Corps Scholarship for Service program as well as various graduate and postdoctoral programs.
    - Developing a coordination mechanism linking Federal cybersecurity and computer forensics training programs; and
    - Establishing IT security programs for departments and agencies, including awareness, audits, and standards.

- **Joint DHS/Treasury Computer Investigative Specialist Program:** Provides training for criminal investigators in basic computer forensics through a basic six-and-a-half week course.

Other Federal agencies also offer training courses related to CI/KR protection. These include:

- **OPM Critical Infrastructure Protection Program:** A four-and-a-half day seminar designed to present information on CI/KR targets including communications, utilities, transportation, banking and finance, and the public health system.
- **DOD Critical Infrastructure Protection Training and Resources:** A series of educational programs and CI/KR protection-related resources designed to help inform Department of Defense (DOD) and other Federal agency personnel on CI/KR protection.

DHS will solicit recommendations from national professional organizations and Federal, State, Territorial, tribal, local, private sector, and nongovernmental security partners for additional discipline-specific technical training courses related to CI/KR protection and support course development when appropriate.

6.2.4.3 Standards for Education and Professional Competency

Professional and continuing education and training programs are important tools for ensuring the effective use of a complex and technologically sophisticated workforce. CI/KR protection involves many skills and professions that already have developed education, training, and certification systems through professional organizations or government licensing. The CI/KR protection field also involves unique skills and professional expertise that have yet to incorporate such training and certification mechanisms into a nationwide system. DHS will focus on these unique skills and expertise to ensure that a skilled workforce is available over the long term to implement the NIPP.

For example, DHS is collaborating with the Department of Defense to guide the development of a national certification program that includes a comprehensive set of information technology job skills standards for security professionals within the Federal Government and private industry. DHS will encourage and, when appropriate, facilitate the development of similar professional and surety standards for the remaining six areas of unique and critical CI/KR protection expertise specified above.

6.2.4.4 Academic and Research Programs

DHS will help business graduate programs to incorporate CI/KR protection into business school programs. For example, DHS is coordinating with universities to incorporate security-related curriculum into business school programs under Project MBA, a new training program currently under development. The goal of Project MBA is to better prepare the Nation's future business leaders to plan, implement, and manage protective measures programs for private sector critical infrastructure.

DHS will examine existing cybersecurity programs within the research and academic communities to determine their applicability as models for CI/KR protection education and broad-based research. These programs include the following:

- Co-sponsorship of the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program with the National Security Agency (NSA).
- Collaboration with the NSF to cosponsor the Scholarship for Service (SFS) program, also known as the Cyber Corps program. The SFS program provides grant money to selected CAEIAE and other universities with programs of a similar caliber to fund the final 2 years of student bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.

DHS will ensure that the CI/KR Protection R&D Plan appropriately considers the human capital needs for protection-related R&D by incorporating analysis of the research community's future needs for advanced degrees in protection-related disciplines into the plan development process.

6.2.4.5 Organizational Training and Exercises

DHS will facilitate the development of national standards, guidelines, and protocols for incident management training and exercises that include CI/KR protection evaluation to ensure that exercise programs include adequate testing of CI/KR "steady-state" protective measures and plans.

DHS will ensure that the NIMS Integration Center, which serves as the repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, regularly includes information on CI/KR protection best practices.

6.3 Research and Development to Improve Protective Capabilities

6.3.1 The National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with Director of the Office of Science and Technology Policy (OSTP), Executive Office of the President, to develop the annual National Critical Infrastructure Protection Research and Development Plan (NCIP R&D Plan) as a vehicle to support implementation of CI/KR risk management and other protection efforts.

The NCIP R&D Plan provides the focus and coordination mechanisms required to achieve the vision provided in the President's Physical and Cyber CI/KR Strategies. That vision calls for a "systematic national effort to fully harness the Nation's research and development capabilities." The R&D planning process is designed to address common issues faced by the various sector security partners and ensure a coordinated R&D program that will yield the greatest value across a broad range of interests and requirements. The planning process also provides for the revision of research goals and priorities to respond to changes in the threat, technology, and other factors.

6.3.1.1 R&D Plan Development

DHS and OSTP coordinate with Federal, private sector, academic, and national laboratory security partners during the R&D planning cycle to focus on both physical and cyber CI/KR protection. The NCIP R&D Plan articulates strategic goals and needed advances in CI/KR protection capabilities against which current and planned risk management and protection initiatives are evaluated and gaps identified. It then defines a program of CI/KR protection-related technology development initiatives to meet the needs and fill the gaps.

The interagency process used to develop and coordinate this plan is managed through the Infrastructure Subcommittee of the NSTC, which is co-chaired by DHS and OSTP. SSAs are responsible for providing input into the plan after coordination with sector representatives and experts through such bodies as various sector-specific SCCs and GCCs.

6.3.1.2 Directing the Development of CI/KR Protection Technologies

The NCIP R&D Plan will use the three-step approach described in this section to direct the development of CI/KR protection-related technologies to meet existing and future requirements:

Step 1: Identify CI/KR Protection R&D Strategic Goals and Objectives

NCIP R&D planning process has identified three long-term strategic goals and provided direction to the R&D community through a prioritized CI/KR protection agenda. The three strategic R&D goals for CI/KR protection include the following:

- A *common operating picture architecture* CI/KR that will integrate infrastructure monitoring and support systems with data collection, processing, analysis, and visualization capabilities to provide real-time, analysis and reports on the status and security of the country's CI/KR;
- A *next generation Internet architecture* with "designed-in security" that is more secure than the existing Internet. The architecture will incorporate security and protection measures at all levels from the basic hardware components through all layers of software as an explicit design feature of this new network rather than adding it later as a post-development patch; and
- *Resilient, self-diagnosing, self-healing systems* that if attacked or damaged can manage or contain the extent of damage, continue to provide critical services, and adapt and self-heal damaged areas.

The strategic goals identified in the NCIP R&D Plan are used to inform Federal R&D investment decisions and also to provide a coordinated approach to the Federal research program. DHS S&T and OSTP will work with the Office of Management and Budget (OMB) to use the R&D Plan as a decision tool for evaluation of budget submissions across Federal agencies. These goals also help define the research programs of research performers who receive Federal grants and contracts for research.

Step 2: Identify CI/KR Protection R&D Themes

Science and technology needs for CI/KR protection programs fall into nine topical areas or themes that cut across all CI/KR sectors. Focusing research on these areas enables the development of effective solutions that may be applied across sectors and disciplines. These themes also provide an organizing framework for the SSAs during the development of the R&D requirements for their sectors, which will be reported in their SSPs. These requirements specify the capabilities each sector needs to satisfy CI/KR protection needs. By incorporating these requirements into the NCIP R&D Plan, OMB is better able to ensure that agency R&D budget requests are aligned with the national R&D plan for CI/KR protection. The themes are:

- **Detection and Sensors Systems:** Selection, placement, and integration of systems to detect WMD intrusion, small arms, intent, and humans (actors and victims). The research plans for certain sensors and detectors reside within several R&D communities, specifically for chemical, biological, radiological, nuclear and explosive agents. The standards community also has a role in fostering interoperable sensor systems and in establishing performance specifications;
- **Protection and Prevention Systems:** Devices, methods, and processes that prevent damage or destruction of CI/KR and their interconnections. This theme involves layers of defensive measures that deter attackers, prevent entry, inhibit the use of weapons and harden infrastructures;
- **Entry and Access Portals:** Devices, systems, and methods that control access to CI/KR. The types of portals include physical entryways and communications nodes. The objects of interest passing through portals include people, vehicles, goods, cargo and freight, electronic information, and communications. The enabling technologies include biometric identification and automated identification methods such as radio frequency tags, sensor data, and x-ray interrogation systems;
- **Insider Threat Detection:** Profiling, detection, anticipation, and monitoring of activities of trusted persons or automated entities with access to a critical asset, whether central or distributed. This theme focuses on detecting malicious intent, monitoring activities to identify anomalies and early indicators, and prevention and protection through real-time auditing of systems and layered measures to prevent inappropriate actions;
- **Analysis and Decision Support Systems:** Modeling, simulation and analysis, and decision support tools to analyze the complex systems and situations found in terrorist attack scenarios, including dependencies and interdependencies among sectors. This theme is of ubiquitous importance across

sectors because CI/KR assets are highly interdependent. Systems to be developed include risk-based prioritization and investment strategy aids; vulnerability assessment tools; modeling and simulation of sector operations, interconnectivity, and the consequences of attacks; and response planning tools to simulate scenarios and evaluate candidate responses;

- **Response, Recovery, and Reconstitution Tools:** Systems, devices, and processes that support first responders and those building temporary and permanent replacements of damaged infrastructure, and the planning systems for all such efforts. Associated technologies include equipment to detect victims and assess safety hazards, simulation tools for response planning and training, and self-recovery design for cyber systems;
- **Emerging Threats and Vulnerabilities Analysis Aids:** Methods and processes that enable early discovery of emerging threats and vulnerabilities or the potential of adversaries to present new threats. Many emerging physical threats relate to changes in the lethality, delectability, or resistance to countermeasures of WMD agents. New cyber threats include those with the capability to attack a wide range of networks;
- **Advanced Infrastructure Architectures:** Use of new technology and associated designs that address current and future infrastructure needs with replacements that are inherently more secure. Greater inherent security can rely on automatic responses to attacks, self-healing features, and co-design of physical and cyber components that can prevent, respond to, or recover from attacks more quickly than current systems. Such improvements can have important dual-use benefits, with systems better able to respond to minor but frequent accidental events that degrade performance; and
- **Human and Social Issues:** Research into behavioral issues related to victim response and infrastructure operator actions to enhance understanding and decisionmaking during a terrorist event. The focus areas for this theme include coordination among government and private sectors, user-centered designs, the resiliency of commercial enterprises and the economy, and risk communication and management.

Step 3: Establish the NCIP R&D Technology Roadmap

The NCIP R&D Technology Roadmap provides a way for Federal managers such as DHS, OSTP, OMB, and the SSAs to coordinate infrastructure protection R&D across the diverse set of CI/KR protection security partners. This Roadmap provides a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements. It also provides a systematic way to determine interrelationships among other R&D programs, both public and private.

6.3.2 Cyber Threat R&D Planning

The Cybersecurity R&D Act authorized a multiyear effort to create more secure cyber technologies, to expand cybersecurity R&D, and to improve the cybersecurity workforce.

To further address cyber R&D needs, OSTP established a Cybersecurity and Information Assurance Interagency Working Group (CSIA IWG) under the NSTC. The CSIA IWG was jointly chartered by the NSTCs Subcommittee on Networking and Information Technology Research and Development (NITRD) and the Subcommittee on Infrastructure. The Director of Cybersecurity R&D in the DHS Science and Technology (S&T) Directorate co-chairs this interagency working group, which includes participation from 20 organizations in 11 departments and agencies, as well as from several offices in the White House. The purpose of the working group is to coordinate policy, programs, and budgets for cybersecurity and information assurance R&D.

The CSIA IWG currently is engaged in developing the Federal Plan for Cybersecurity R&D, which includes near-term, mid-term, and longer term cybersecurity research efforts, in response to the *National*

Strategy to Secure Cyberspace and HSPD-7. Specific examples include efforts to improve the security of fundamental protocols (such as Internet Protocol version six) and authentication technologies and periodically review emerging technologies. DHS actively participates in CSIA IWG activities and continues to identify critical cyber R&D requirements for incorporation into Federal R&D planning efforts.

DHS and OSTP also facilitate communication between the public and private research and security communities, to ensure that emerging technologies are periodically reviewed by the appropriate body within the NSTC in the context of possible homeland and cyberspace security implications and relevance to Federal research agenda.

6.3.3 Other R&D that Supports CI/KR Protection

Other R&D efforts, developed in accordance with requirements set forth in the President's Physical and Cybersecurity strategies that will be used to support CI/KR protection are discussed in this section.

6.3.3.1 Interoperable Standards to Ensure Compatibility of Communications Systems

SAFECOM, a program in the DHS S&T Directorate's Office for Interoperability (OIC), serves as the Federal umbrella to promote and coordinate initiatives between local, State, Territorial, and tribal entities to improve public safety response through more effective and efficient interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and to create standards, models, and solutions to help meet those requirements.

SAFECOM's role in standards development is to:

- Support existing or, where necessary, establish a voluntary consensus process that meets the current security environment, identifies and implements the needs and requirements of public safety, and maximizes flexibility and innovation; and
- Develop near-term tools that can maximize the efficiency of public safety technology, such as recommended models for statewide planning, criteria for creating governing bodies, standard operating procedures, grant guidance, and communications-specific exercise methodologies.

The following are key characteristics of SAFECOM's approach to facilitating the development of national voluntary consensus standards for public safety interoperable communications:

- Implements a practitioner-driven approach;
- Applies a comprehensive framework which utilizes a structured lifecycle approach that employs continuously evolving common grant guidance to assist communities in planning and implementing their interoperability solutions;
- Integrates new and legacy systems using a "system of systems"; and
- Establishes industry and government partnerships.

6.3.3.2 Explore Methods to Authenticate and Verify Personal Identity

In coordination with a number of Federal agencies, DHS funds several R&D programs relating to authentication and verification of personal identity for the CI/KR workforce. Examples include research into the protection of physical infrastructure by authentication of network users, recommendations from the private security guard industry on legislative measures needed to achieve progress in the area of personnel surety, and advances in basic research.

Additionally, DHS worked with the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST) to establish a Homeland Security Standards Panel (HSSP)

that has been coordinating the development of consensus standards among the 280 different standards development organizations.

6.3.3.3 Improve Technical Surveillance, Monitoring and Detection Capabilities

Advances in surveillance, monitoring and detection increase the Nation's ability to find threats in the making rather than responding to an attack after the fact. From an R&D perspective, advanced processing of digital video, and other data collection methods is important in providing information to responsible security forces, in a way that is reliable, practical, and fast. In cooperation with the British, U.S. expertise has been brought to bear on reducing the amount of data that needs to be transmitted by extracting out only that information required for sophisticated analysis. Massive data storage capacity that is small and affordable is also nearing readiness for the market as a result of R&D investments. These advances make better use of the data collection capacity readily available, while providing information to security forces in a more actionable, focused manner.

6.3.4 Technology Pilot Programs

DHS identifies protective gaps and trends common to certain types of assets or geographic areas in the course of conducting site assistance, buffer zone protection visits, and other vulnerability and risk assessments. On occasion, an appropriate technological solution may be the best approach to addressing such gaps. When R&D is required to create or test the appropriate technological solution, the DHS S&T Directorate will work closely with other relevant security partners to implement a pilot program. In some cases, this involves working with the DHS Office of State and Local Government Coordination and Preparedness (OSLGCP) to identify funds and specialized training, while in other cases pilots are implemented using off-the-shelf technology. If the pilot programs are successful, the technological solutions are then implemented in other locations where similar gaps exist. The following are examples of recent technology pilots:

- **National Capital Region Rail Security Corridor Pilot Project:** Designed to meet the needs of local law enforcement, first responders, and the Federal Government while supplementing the existing security measures of freight rail operations in the Washington, DC, area. This pilot project seeks to address security challenges surrounding rail infrastructure and freight traffic through large cities while maintaining fluid rail operations. The pilot project components include a virtual security fence consisting of approximately 200 high-resolution fixed cameras; the use of radio frequency identification (ID) scanners; and virtual gates for chemical and radiological detection. Data from the fence and the gates will be encrypted and transmitted simultaneously to multiple locations, such as U.S. Capitol Police, USSS, the rail corridor's owner/operator, and other applicable Federal or local agencies.

- **Constellation Automated Critical Asset Management System (Constellation/ACAMS) :** Constellation/ACAMS, being developed through a partnership between DHS and the City and County of Los Angeles, encompasses an automated system, tools, resources, and related training to assist in protecting CI/KR located in major urban areas. Constellation/ACAMS enables planning for, responding to, and recovering from catastrophic incidents. As such, it focuses on the unique requirements and information needs of first responders. It possesses a complete reporting capability to answer both local and national data calls on critical assets, including information about location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of buffer zone protection plans and pre-incident operational plans for local police and first responder use.

- **South Florida Coastal Surveillance Prototype Test Bed:** DHS S&T and the U.S. Coast Guard (USCG) planned and funded the South Florida Coastal Surveillance Prototype Test Bed, a port and

coastal surveillance prototype in Port Everglades, Miami, and Key West areas. The evolutionary prototype provides an initial immediate coastal surveillance capability in a high priority area and:

- Offers the means to develop and evaluate concept of operations in a real-world environment;
- Implements and tests interoperability among DHS and DOD systems and networks such as the U.S. Navy/USCG Joint Harbor Operations Center (JHOC);
- Tests and evaluates systems and operational procedures; and
- Becomes the design standard for follow-on systems in other areas and integration with wider area surveillance systems.

6.4 Building and Maintaining Databases, Simulations, and Other Tools

Many databases, simulations, and decision support systems currently exist or are under development to enable the execution of national risk management activities. The databases provide capacity for such functions as maintaining an inventory of asset information and the estimating potential consequences of an attack or incident (e.g., the National Asset Data Base), storing information related to terrorist attacks or incidents (e.g., the National Threat Incident Database), analyzing dependencies and interdependencies (e.g., the Critical Infrastructure Protection Decision Support System), and managing the implementation of various protective programs (e.g., the BZPP Request Database). To be effective, these tools must be updated and in some cases, new tools developed. Priority efforts in this area will be focused on populating and improving key databases, developing and utilizing simulation and modeling, and coordinating with security partners on databases and modeling as described in the following sections.

6.4.1 The National Asset Database

HSPD-7 directs the Secretary of Homeland Security to lead efforts to reduce the Nation's vulnerability to terrorism and deny the use of infrastructure as a weapon by developing, coordinating, integrating and implementing plans and programs that identify, catalog, prioritize, and protect infrastructure in cooperation with all levels of government and private sector entities. In support of the requirement to identify, collect, catalog and maintain a national asset inventory, DHS developed the national Asset Database (NADB), a continually evolving and comprehensive catalog of the assets that comprise the Nation's infrastructure. Also containing descriptive information regarding those assets, the NADB is the primary Federal repository for CI/KR information. Although the NADB is not, in and of itself, a listing of prioritized assets, it has the capability to be queried in a variety of manners that can help inform NIPP implementation and other risk-reduction activities across the 17 CI/KR sectors and throughout the 56 States and Territories.

The current NADB is a scalable, flexible, and modular portal to facilitate evolution, growth, and continued interconnectivity with additional databases and tools. The next-generation NADB will combine multiple commercial and Federal infrastructure databases; vulnerability assessment tools and libraries; intelligence and threat reporting databases; and geospatial tools into a single, integrated, Web-based portal. The NADB and its integrated modules will transform the current fragmented collection of existing tools into a unified, central repository that can support the implementation of NIPP risk management framework activities.

6.4.1.1 First Priority: Populate the NADB

At this time, DHS is focused on populating the current generation NADB to support the development of a national asset inventory which, in turn, will support the development of an informed national risk profile. The types of information desired as well as the means for populating the NADB are described in Chapter 3. In addition to hosting the national asset inventory, the current generation NADB integrates information available in various DHS and other Federal databases using a single portal with a common interface. This

facilitates information sharing among Federal agencies and helps ensure Federal security partners have access to the most complete, accurate, and current information possible. In support of this, many organizational units within DHS that maintain special purpose databases work through the NADB as the official DHS repository of national-level CI/KR information.

The integrated, first-generation NADB supports the following activities:

- Identification and cataloging of key asset and resource information (e.g., specific attributes, vulnerability-related data) necessary for risk-reduction analyses;
- Development of a comprehensive picture of the Nation's infrastructure across all 17 CI/KR sectors;
- Use of a consequence-based prioritization process to identify assets for further focused effort in determining vulnerabilities and subsequent protective measures;
- Integration of a geospatial capability into the NADB portal interface to produce visual displays and screen maps of selected NADB assets on demand; and
- Integration of data and results from various DHS support organizations (e.g., NISAC) through a single portal.

6.4.1.2 Next Priority: Building the Next-Generation Asset Database

In addition to populating the NADB to support the creation of a comprehensive national asset inventory, DHS is developing the next-generation NADB with a more versatile platform to allow for integration of DHS and SSA mission-specific applications and mission specific databases. The goal of this effort is to create an asset database that supports the implementation of NIPP risk management framework activities, including:

- Integration of vulnerability, consequence, and asset attribute data into a single portal interface to be used as the foundation for the NIPP risk assessment process;
- Infusion of threat data to support the development of asset and system risk scores;
- Prioritization of assets and systems across sectors and jurisdictions based on risk to promote the more effective allocation and use of available resources and to inform planning and threat response actions at all levels of government and the private sector;
- Sharing of information so that all partners involved in Homeland Security operate from a common frame of reference with consistent information;
- Acting as a primary information and integration hub for protective security needs throughout the country in support of DHS and SSA-led activities;
- Supporting the efforts of law enforcement agencies during NSSEs and other high-priority security events; and
- Supporting the efforts of primary Federal agencies to respond to and recover from major natural or terrorist-caused disasters.

6.4.1.3 NADB Roles and Responsibilities

Although DHS is ultimately accountable for the success of the Nation's CI/KR protection program, implementation requires an integrated process across all security partners via the NIPP. The same is true for the development and population of the NADB, which is highly dependent on the participation and support of the SSAs and private sector entities.

SSAs are responsible for providing sector infrastructure information to DHS for inclusion in the NADB using the format, data scheme, and taxonomy employed by the NADB.[13] As the responsible agent for the identification of assets and existing databases for their sectors, the SSAs should have outlined in their respective SSPs the plans and processes for sector asset and database identification. The SSAs will also have the lead for working with their sector's private sector security partners to facilitate the collection of accurate information for the population of the NADB.

The most current and accurate CI/KR data is best known by the owners and operators themselves. Thus, as the owners and operators of more than 85 percent of the Nation's infrastructure, private sector entities are encouraged to be actively involved in the population and development of the NADB. Primarily through the provision of asset information and industry-specific subject matter expertise, the private sector is playing an integral role in the development of the NADB.

6.4.2 Simulation and Modeling

DHS will use existing and develop new capabilities as needed to comprehensively model potential consequences of terrorist exploitation of vulnerabilities in CI/KR. It will focus specifically on densely populated areas. The DHS Preparedness Directorate will be the lead for modeling and simulation capabilities for CI/KR protection. In this capacity, it will:

- Coordinate with DHS S&T Directorate on requirements for the development, maintenance, and use of research-related modeling capabilities for CI/KR protection;
- Specify the DHS requirements for the development, maintenance, and use of operations-related modeling capabilities for CI/KR protection; and
- As directed by HSPD-7, SSAs with relevant modeling capabilities will cooperate with DHS to develop appropriate mechanisms for the development, maintenance, and use of relevant modeling capabilities for CI/KR protection.

The U.S.A. Patriot Act of 2001 (P.L. 107-56) established the NISAC to provide advanced modeling and simulation capabilities for the analysis of CI/KR and their interdependencies, vulnerabilities, and complexities. In accordance with the 2002 Homeland Security Act, DHS acts as the program office for NISAC and manages its development, maintenance, and use of relevant modeling capabilities for CI/KR protection.

6.4.3 Coordination with Security Partners on Databases and Modeling

Integrating existing databases into DHS databases such as the NADB not only reduces duplication of effort, but also ensures that available data is consistent, current, and accurate, and provides users with a consolidated picture to view the national infrastructure across all CI/KR sectors—but only if the source information is maintained properly. Properly maintaining a current and useful database involves the support, coordination, and commitment of the SSAs, private sector entities, and other security partners. The effectiveness of the effort depends on all security partners keeping their databases and data systems current. As the responsible agent for the identification of assets and existing databases for their sectors, the SSAs will:

- Outline in their SSPs the sector plans and processes for database, data system, modeling and simulation, development, and updates; and

[13] The format, data schema, and integration processes are outlined in the NADB Standard Operating Procedures (SOP). The DHS/IP taxonomy is the foundation for multiple DHS programs that focus on critical infrastructure such as the NADB and the National Threat Incident Database, and should be the foundation outlined within the SSPs. This common framework will allow more efficient integration and transfer of information, as well as a more effective analytical tool for comparison.

- Specify a regular schedule for maintenance and update of databases.

DHS will work with SSAs and other security partners to:

- Identify databases and other data services that will be integrated with CI/KR protection databases and data systems;
- Facilitate the actual integration of databases or importation of data into CI/KR protection databases and data systems, using a common and standardized format, data scheme, and categorization system or taxonomy specified by DHS; and
- Define the schedule for importing databases into such systems as the NADB. Initial milestones for this schedule include identifying additional commercial and Federal databases for inclusion by February 2006 (same deadline as SSPs), and incorporating these additional databases into NADB one year after their identification (February 2007).

6.5 Ongoing Plan Management and Maintenance

6.5.1 Plan Coordination

The NIPP uses the Senior Leadership Council, the Government Cross-Sector Council and the Private Sector Cross-Sector Council as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation and ongoing management and maintenance of the NIPP and SSPs.

In accordance with HSPD-7 paragraph 34, all Federal departments and agencies developed and submitted to the Director of the OMB plans for protecting the physical and cyber CI/KR assets that they own or operate. Since this was a one-time requirement that preceded the establishment of the NIPP, information reported in these plans will be used by DHS and SSAs to inform the NIPP process as appropriate. Agencies will coordinate with DHS whenever information reported in these plans is changed to ensure that the most up-to-date information is considered for NIPP implementation, update, and maintenance.

6.5.2 Plan Maintenance

DHS is the Federal executive agent for NIPP management and maintenance.

The NIPP is a multiyear plan describing mechanisms for sustaining the Nation's "steady-state" protective posture. The NIPP and its component SSPs include a process for annual review, periodic interim updates as required, and regularly scheduled full reviews and re-issuance every 3 years or more frequently if directed by the Secretary of Homeland Security.

DHS/IP will govern the review and maintenance process for the NIPP; SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to coordinate this effort for their respective SSPs. The NIPP and SSP revision processes will include developing or updating any documents necessary to carry out NIPP activities. The NIPP will be reviewed at least annually to:

- Measure accomplishments in support of program goals and objectives;
- Ensure that the plan adequately reflects the level of resources available and budgeted;
- Adjust activities and initiatives based on a strategic analysis; and
- Incorporate lessons learned and best practices from exercises and actual incidents and alerts.

As changes to either the NIPP or the SSPs are warranted, periodic updates will be issued. Types of developments that merit a periodic update include:

- New laws, executive orders, Presidential directives, or regulations; and

- Procedural changes to NIPP and SSP activities based on real-world incidents or exercise experiences.

The following paragraphs establish procedures for interim changes and full updates of the NIPP and SSPs:

- **Types of Changes:** For the NIPP and SSPs, changes include additions of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in statute, Executive order, or regulation.
- **Coordination and Approval:** Any department or agency with assigned responsibilities under the NIPP may propose a change to the plan. DHS is responsible for coordinating all proposed modifications to the NIPP with SSAs and other security partners as required. DHS will coordinate review and approval for proposed modifications as required. The SSA, in coordination with the GCC and SCC, is responsible for implementing all proposed modifications to the SSPs.
- **Notice of Change:** DHS will issue an official Notice of Change for each interim revision to the NIPP. The SSAs will coordinate with DHS to issue an official Notice of Change for each interim revision to the SSPs. The notice will specify the date, number, subject, purpose, background, and action required, and provide the change language on one or more numbered and dated insert pages to replace the modified pages in the NIPP or SSP. After publication, the modifications will be considered part of the NIPP or SSP for operational purposes pending a formal revision and re-issuance of the entire document. Interim changes can be further modified or updated using this process.
- **Distribution:** DHS will distribute Notices of Change to all participating security partners. Notices of change to other organizations will be provided on request. For the SSPs, the SSA and DHS will distribute Notices of Change to all relevant security partners.
- **Re-issuance of the NIPP:** DHS will coordinate full reviews and updates of the NIPP and component SSPs every 3 years, or more frequently if the Secretary deems necessary. The review and update will consider lessons learned and best practices identified during implementation in each sector and incorporate the periodic changes and any new information technologies. DHS and SSAs will distribute revised NIPP and SSP documents for interagency review and concurrence.

6.6 Key Implementation Actions

All milestones are specified with respect to the date of final signature of the NIPP. If agencies are not able to meet milestones, they should notify the Secretary of Homeland security in a letter specifying the reason and the date by which they will be able to achieve the milestone.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
6.1 Building a Program for National Awareness								
DHS	Identify and assess the requirements for a national awareness program.		X					
DHS	Organize and convene an interagency national public awareness workgroup.		X					
DHS	Conduct inventory of existing national public awareness efforts or partnerships that could support the delivery of messages to broad audiences.			X				

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
DHS	Develop draft NIPP National Awareness Plan for circulation and review with security partners.				X			
DHS	Approve final draft and begin implementation of the NIPP National Awareness Plan.				X			
DHS SSAs SPs	Develop and implement NIPP National Awareness Plan.						X	
DHS	Develop increased awareness to educate CI/KR owners and operators of the risks associated with cyber attacks and to provide the motivation for sufficient investment in cybersecurity programs.							X
6.2 Education and Training								
DHS SSAs	Review a sampling of special, technical, professional, academic, exercise training programs to ensure they are consistent with NIPP requirements.			X				
SPs	Provide recommendations for special, technical, professional, academic, and exercise training program revision to conform to NIPP requirements.				X			
PS	Recommend review and revision of special, technical, professional, academic, and exercise training programs to conform to NIPP requirements.						X	
6.3 Research and Development to Improve Protective Capabilities								
DHS OSTP SSAs GCCs SCCs	Establish industry assessment processes to gather information on industry advances in CI/KR protection-related science and technology.			X				
DHS OSTP	Convene discussions/workshops with security partners to determine CI/KR R&D priorities.				X			
DHS OFA	Develop a database of R&D investments related to CI/KR protection.				X			
DHS OSTP SSAs	Conduct first annual review and issue CI/KR protection R&D plan updates.					X		
DHS SSAs	Identify the universe of CI/KR related R&D databases.						X	
DHS OSTP	Develop architecture for CI/KR protection R&D data collection to guide and monitor R&D efforts and progress relevant to CI/KR protection.						X	

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
DHS	Share appropriate threat information with the CI/KR protection and sector R&D communities to guide emphasis and timing of the future R&D activities.							X
6.4 Building and Maintaining Databases, Simulations, and Other Tools								
DHS SPs	Identify universe of CI/KR related databases.						X	
DHS	Incorporate information contained in relevant CI/KR databases into single CI/KR database (i.e., NADB).							Within 1 year of database ID
6.5 Ongoing Plan Management and Maintenance								
DHS SSAs	Conduct a full review and re-issuance of the NIPP and SSPs to consider lessons learned and best practices identified during implementation as well as any new technologies.							Every 3 years
DHS SSAs	Conduct an annual review of the NIPP and SSPs to identify changes that warrant the development and issuance of a periodic update (e.g., new laws, orders, procedures, etc.).						X	
DHS OFA	Update CI/KR R&D plan.						X	
Key: GCC = Government Coordinating Council, PS = Private Sector, SCC = Sector Coordinating Council, SSA = Sector-Specific Agency, SP = Security Partner, OSTB = White House Office of Science and Technology Board, OFA = Other Federal Agency.								

1

7 Resourcing the CI/KR Protection Program

The President's Homeland Security Strategy established the requirement for DHS to unify America's CI/KR protection efforts and to develop a national infrastructure protection plan to inform the "annual process for planning, programming, and budgeting" of CI/KR protection activities.

The NIPP, therefore, defines a program management approach that provides for:

1. Collecting and validating CI/KR sector requirements;
2. Prioritizing the allocation of Federal resources through the annual budget process;
3. Measuring national results and performance; and
4. Continuously improving CI/KR protection based on results and performance.

This chapter of the NIPP details a process for implementing the second requirement identified above, In addition to DHS, implementation of this requirement involves multiple Federal agencies, the Homeland Security Council (HSC), and the Office of Management and Budget (OMB). This process informs decisions affecting Federal Government programs and Federal grants to State, Territorial, tribal, and local government entities, and influences private sector CI/KR protection investments.

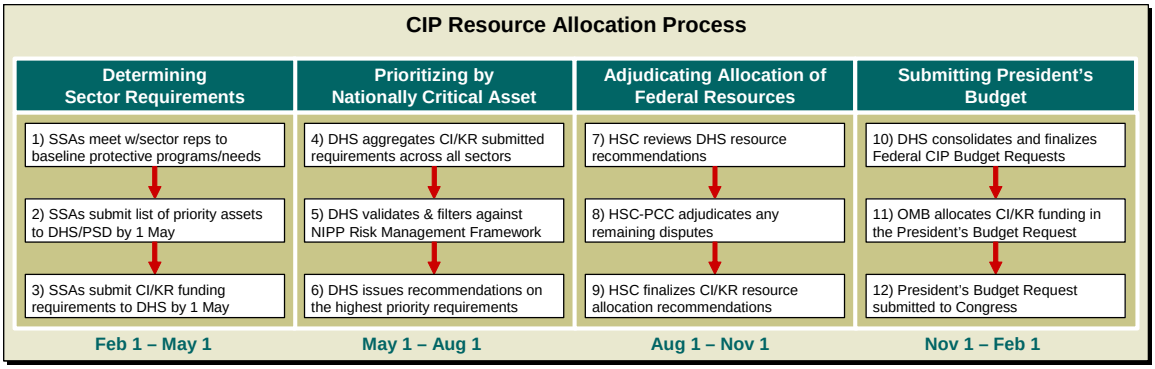


Figure 7-1. Resource Allocation for CI/KR Protection Funding in the President's Budget

As shown in figure 7-1, the resource allocation process for CI/KR protection funding includes four phases. The process starts with establishing sector requirements. The next step involves prioritizing these requirements based on their criticality to the Nation. Protective programs then are recommended that have the greatest potential to reduce the risk as determined through the NIPP risk management framework. The HSC then reviews proposed funding, resolves remaining issues, and finalizes recommendations to be passed to OMB for inclusion in the President's budget submission. Each of these phases is tied to a specific date in the annual budget process and is discussed in detail in the sections below.

7.1 Determining Sector Requirements

The costs of maintaining, improving, and investing in future CI/KR protection activities are expected to grow and continue to present funding challenges for all levels of government and private industry. Since the September 11, 2001 attacks, most NIPP security partners—both in government and the private sector—have increased expenditures to protect physical and cyber CI/KR. Effectively managing the funding of CI/KR protection programs presents a number of issues across a range of sources that include:

- DHS funding for CI/KR protective programs or related grants to the States;
- SSA funding for sector-specific CI/KR protection programs;

- Other Federal agency funding directly or indirectly related to CI/KR protection;
- State and local funding for homeland security programs related to CI/KR protection; and
- Private sector expenditures for security measures to enable CI/KR protection.

The NIPP provides a unified process to enable DHS and its public and private sector security partners to work together in formulating a coordinated allocation of resources from these various funding streams to protect CI/KR. These partners also make independent decisions regarding the use of their own funding authority and resources. The programs these partners fund make important contributions to the overall CI/KR protection mission.

Earlier chapters of the NIPP articulated how DHS and the SSAs will work with the respective CI/KR sectors to determine risks and identify the assets that are deemed nationally critical. As a first step in the resource allocation progress, the SSAs assume the lead role in determining top priorities and specific needs within their sector. Based on guidance from DHS, each SSA develops and maintains current an SSP that supports the goals and objectives of the NIPP. Also, each SSA, using the NIPP risk management framework, will develop and submit to DHS by **April 1** of each year a list of sector priorities and resource needs for CI/KR protection These inputs will be used to justify and rationalize the allocation of Federal resources within each sector and across the Federal Government and will include a:

- Description of the overall sector strategy and programs, and how they achieve the national policy objectives set forth in HSPD-7, the NIPP and other policy documents
- Baseline of existing programs and capabilities in the sector, how they are funded and executed, and how they address national priorities;
- Description of major sector objectives, gaps between current and desired sector capabilities, and a set of proposed programs/initiatives, to include funding priorities based on risk; and
- Metrics to be used to assess progress and return on investment.

7.2 Prioritizing by National Critical Asset

DHS, in its role as overall coordinator for CI/KR protection at the national level, is responsible for identifying nationally critical assets. With finite Federal resources dedicated to protecting CI/KR, a comprehensive, coordinated review of all Federal CI/KR activities in this area is needed to ensure a uniform decisionmaking process that prioritizes Federal investments and makes informed trade-offs. DHS will work closely with the Executive Office of the President (e.g., HSC, OMB) to aggregate department and agency requests. DHS recognizes the need to balance a dual priority: (1) collaborating effectively to prioritize funding across DHS, SSAs, and other Federal agencies and (2) integrating efforts that assess the relative priority of nationally critical assets that, in turn, determine CI/KR protection requirements.

In the second step of the resource allocation process, DHS receives each Sector's list of priorities and resource needs, aggregates the submissions, and analyzes CI/KR sector information against the risk management framework to determine which assets are considered nationally critical and which programs will have the greatest potential to reduce overall national-level risk. Based on this analysis, DHS will develop programmatic and budget recommendations that direct Federal CI/KR protection resources to those areas of greatest risk and need (e.g., those areas that manage and mitigate the greatest risks to CI/KR).

DHS recommendations then are forwarded to the Homeland Security Council for policy review, coordination, and (as necessary) adjudication and deconfliction. These recommendations provide the HSC with a complete picture of the risks facing the Homeland, the associated Federal CI/KR protection spending requirements including a description of how the funding proposal addresses overall national priorities,. DHS will provide its recommendations to the Homeland Security Council by **August 1** of

every year for the fiscal year 2 years hence (e.g., analysis in FY2006 will affect FY2008 programs). Figure 7-2 highlights the timing of DHS recommendations and how they fit into the Federal Budget Cycle.

7.3 Adjudicating Allocation of Federal Resources

DHS will submit its proposed recommendations on Federal resource allocation across the U.S. Government in support of national CI/KR protection missions, goals, and objectives to the HSC for review by **August 1** of each year. In its recommendations, DHS will explain how its proposed course of funding best addresses national priorities. The HSC will review the recommendations and, as necessary, convene the HSC Critical Infrastructure Protection Policy Coordinating Committee to address any outstanding policy or budgetary issues requiring interagency coordination and approval. Ultimately, the HSC will act as the final policy arbiter for funding decisions related to Federal CI/KR protection programs. By **November 1** of each year, the HSC will conclude the approval process for the Federal CI/KR protection budget allocations and DHS, in coordination with the HSC, will submit a synopsis of the proposed Federal CI/KR budget to OMB for use in building the proposed CI/KR protection budgets for DHS and the other SSAs. This synopsis will include:

- Summary of national CI/KR protection goals and objectives;
- A description of overall and sector-specific programs recommended for funding;
- An explanation of the rationale for prioritized funding in terms of reducing national risk; and
- Metrics used to measure progress, performance, and expected return on investment.

This synopsis will provide background information and justification that OMB can use to inform decisions on CI/KR protection funding levels in the context of the overall Federal budget. Each SSA's CI/KR protection program is weighed against other programs within its department or agency for funding levels within the budget. This synopsis also provides the overarching and unifying context for OMB as it scores and weighs the funding level of CI/KR protection programs within an SSA's overall President's budget request.

Figure 7-2 provides a summary timeline that illustrates how the phases of this budget process relate to one another and when they take place during a typical year.

7.4 Grant Monies for Infrastructure Protection

The above process focuses explicitly on those programs and initiatives funded by DHS and the SSAs. Each SSP will include a list of priority programs that the sector, with input from the SCC and GCC, deems crucial to improving its risk posture. In some instances, however, those programs may not be considered or ranked as high priority from a national perspective. In these instances, States may seek a secondary source of Federal funding to address their priority CI/KR protection programs through the use of various grant programs.

The homeland security grants process is the primary means available to States and local agencies to develop their preparedness capabilities and represents a key link between Federal, State, Territorial, tribal, and local CI/KR protection programs. Specifically, homeland security grants provide an avenue for directing Federal resources to CI/KR needs which are more appropriately handled and managed by State and local entities. The DHS Office of State and Local Government Coordination Programs (OSLGCP) was established, in part, to help States, Territories, tribal, and local authorities use Federal homeland security grants programs to enhance their ability to prevent, protect, respond to, and recover from acts or threats of terrorism and other hazards. OSLGCP offers access to significant funding through several grant programs that can be leveraged to meet infrastructure protection needs. These programs include:

- **Targeted programs:** Grants for BZPP and specific activities focusing on ports, mass transit, rail transportation, etc., fall into this category.
- **Thematic programs*:*** Grants for a broader set of activities that support the HSPD-8 mission areas, SLGCP's target capabilities, or the national priorities fall into this category.

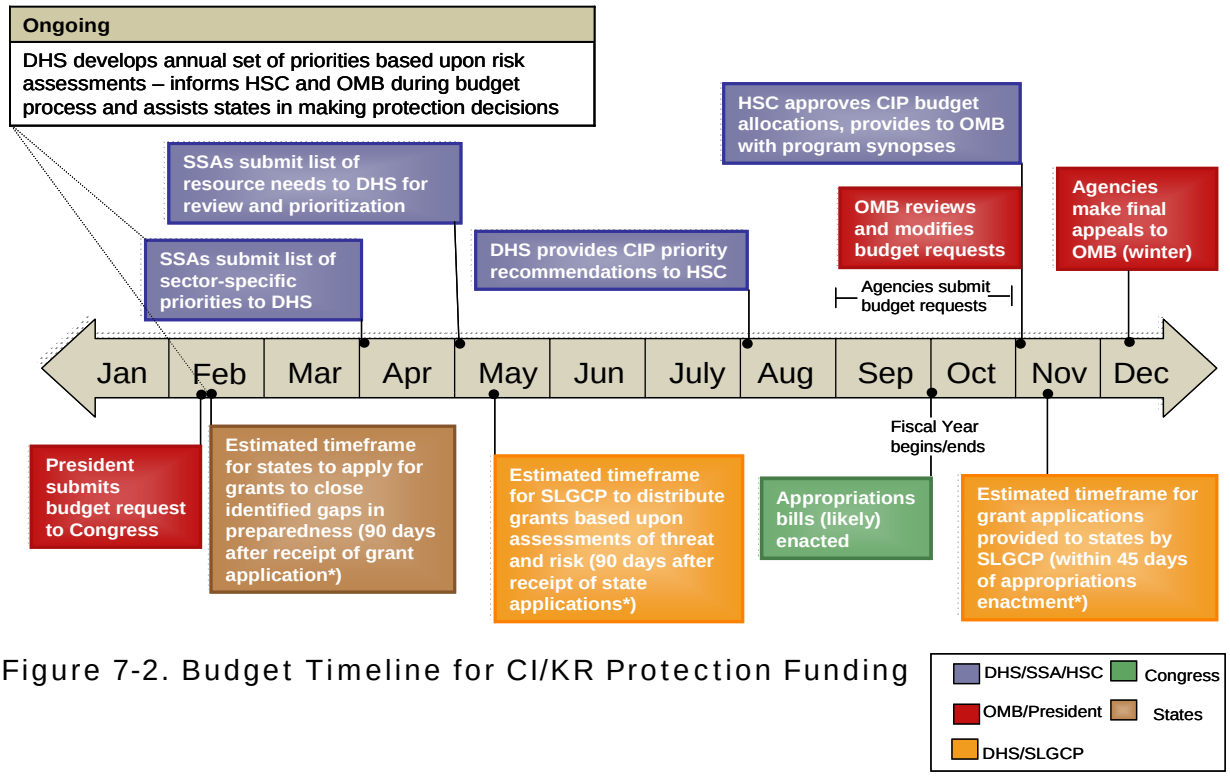


Figure 7-2. Budget Timeline for CI/KR Protection Funding

Allocations are made both on the basis of risk (e.g., those areas most exposed to risk) and need (e.g., identified gaps or shortfalls). DHS grant programs, while broadly defined as "homeland security" in scope, can be used to support infrastructure protection needs. These specific programs include, but are not limited to:

- Homeland Security Grant Program (including the State Homeland Security Program, Urban Areas Security Initiative, and Law Enforcement Terrorism Prevention Program);
- Buffer Zone Protection Program (managed in conjunction with the DHS/OIP);
- Transit Security Grant Program;
- Port Security Grant Program; and
- Intercity Bus Security Grant Program.

In FY2005, States and urban areas are aligning their homeland security strategies with the seven National Priorities included in the Interim National Preparedness Goal. These strategies, therefore, will explicitly link with two National Priorities that are directly related to infrastructure protection efforts: implementing the NIPP and enhancing regional collaboration. Through the Governor-appointed SAA, which serves in each State as the lead for program implementation, States will identify and prioritize requirements for homeland security. Individual CI/KR sectors, State governments, local and tribal authorities, and regional consortiums can all leverage assistance from these funding streams to accomplish the highest priorities as

identified in their strategies and through the strategic planning process. In FY2006, States and local agencies will again be asked to assess and update their needs and capabilities, which will drive their DHS grant funding requests.

As part of this effort, DHS will provide State, Territorial, tribal, and local authorities with guidance on how to assess CI/KR protection needs and programs as they for apply grants resources. This will represent a powerful tool in leveraging the full range of Federal resources to accomplish national and/or CI/KR sector goals and objectives. [Note: additional information on OSLGCP grant programs, guidelines, allocations, and eligibility are available at: http://www.ojp.usdoj.gov/odp/.]

7.5 Risk-Based Resource Allocation

As stated above, the NIPP uses a risk-based approach to drive decisions regarding allocation of resources to CI/KR protection activities at all levels of government and within the private sector. The use of funding to support CI/KR protection programs is based on a straightforward principle: *directing resources to areas of greatest priority in order to effectively manage risk.* Funds are directed towards protective programs that are assessed to have the greatest potential to reduce the risk to critical infrastructure.

Figure 7-3 summarizes how identifying and prioritizing nationally critical assets informs the Federal Budget and grant processes. National, sector, and State CI/KR protection resource allocation decisions should all reflect similar priorities based on an evaluation of critical assets and the risk to those assets. Each level of allocation decisions (Federal, State, Territorial, local, tribal, and private sector) ultimately plays a role in the successful execution of the NIPP.

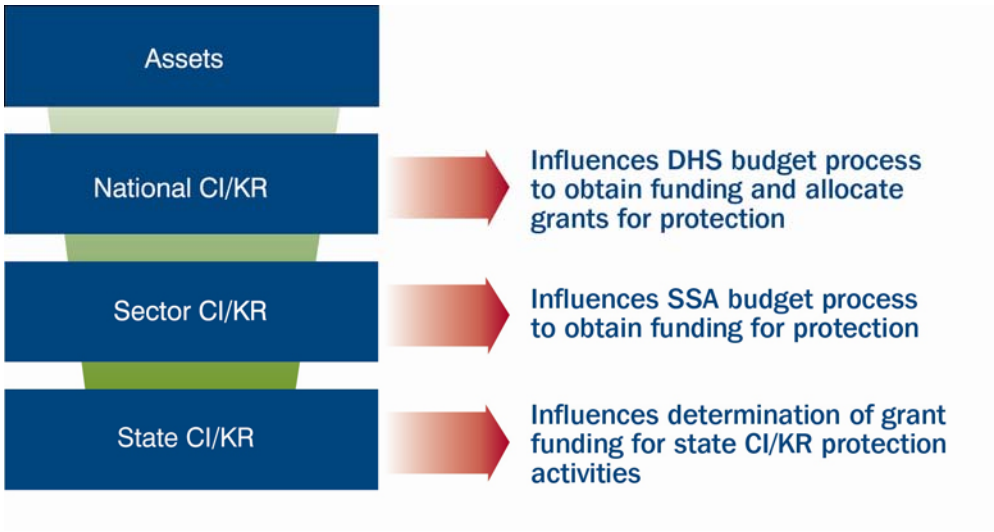


Figure 7-3. How Nationally Critical Asset Priorities Inform the Budget and Grant Process

7.5.1 Leadership and Setting the Agenda for Risk Reduction

The priorities for CI/KR protection set forth in the national strategies, statutes, and Presidential Directives identify key areas that must be targeted for risk reduction. These priorities will change over time as the underlying threats change and as the overall level of preparedness improves. Reducing the risks to critical infrastructure will require not only that the U.S. Government apply funding to a range of public and private sector needs, but also that DHS, SSAs, and State, Territorial, tribal, and local governments work closely with private industry to promote the most efficient expenditure of voluntary resources by asset owners and operators. The methods for carrying out this coordination include setting a national agenda for CI/KR protection and creating the framework that enables other security partners to collaborate with one another.

7.5.1.1 Setting an Agenda in Collaboration with CI/KR Protection Security Partners

Pursuant to HSPD-7, the Secretary, as "the principal Federal official" for protection of the Nation's CI/KR, is responsible, in coordination with other security partners, for setting the agenda, determining which regulatory authorities exercised by the various Federal agencies are appropriate for supporting the national CI/KR protection program, and setting priorities for funding by all security partners.

7.5.1.2 Enabling Collaboration Between Other Security Partners

The NIPP uses the risk management framework to enable coordination between security partners beyond the Federal Government. Coordination between State and local agencies and the sectors themselves ensures that cross-sector impacts and priorities are accurately identified and understood. Each step of the risk management framework presents unique opportunities for collaboration. Table 7-1 highlights these opportunities and demonstrates where Federal, State, Territorial, tribal, local, and private sector resources can be leveraged.

Table 7-1. Opportunities for Funding Collaboration

Step	Opportunities for Collaboration	Resource Implications
Set Security Goals	The development of security goals requires input from private sector owners/operators in order to determine what posture will be sustainable. Including the State and local perspective will add even more realism on the availability of local resources and the concerns of the populations in areas where physical assets are located.	Funding for the development of security goals is usually limited. However, planning at this stage is critical in ensuring that resource use is maximized.
Identify Assets	While SSAs and their security partners can identify assets with potentially significant consequences based on the attributes of the specific asset, those at the State and local level can often provide much greater insight on interdependencies and co-location of assets that increase their potential significance. SSAs should integrate asset information with the NADB to help ensure a common operational picture of infrastructure assets.	Various funding has been made available to DHS, SSAs, and States to assist in their identification and characterization of assets, and in the assessments of those assets (see below).
	Federal, State, Territorial, tribal, and local agencies have also undergone several rounds of asset identification.	
	In the long term, State, Territorial, tribal, and local agencies can assist by tracking changes that may occur to State-owned or operated infrastructure or in terms of increased populations around certain sites.	
	Private industry plays a role in this process, assisting Federal, State, Territorial, tribal, and local agencies in identifying CI/KR.	
Assess Risks	A variety of Federal, State, Territorial, tribal, and local agencies often monitor selected assets and may apprehend individuals or groups for a variety of related or unrelated activities prior to any type of attack occurring. Thus, they play an important part in informing the threat picture at any one time.	Homeland Security Grants, BZPPs, SAVs, port facility vulnerability assessments, and other types of security reviews provide information for the assessment of risks. These activities are generally funded through the States.

Step	Opportunities for Collaboration	Resource Implications
	Insights into interdependencies will allow potential consequences to be more accurately estimated—as will knowledge of local conditions that may increase or decrease consequences. In some instances, State and local agencies may already have conducted consequence assessments for emergency planning and exercises.	By coordinating with SSAs, the States will be able to allocate their resources where they are most needed (due to risk levels or lack of funds for facility or system assessments). Similarly, the SSAs will help ensure that time is not wasted through redundant reviews.
	Past exercises and assessments, as well as local knowledge of individuals and facilities, can contribute to the assessment of vulnerabilities.	
	Local officials are most aware of local emergency response resources and capabilities should an event occur.	
	The SSAs, working with private industry, may have the best information on the operations inside any particular system, building or facility, but the State and local perspective will be invaluable for information "outside the fence."	
Prioritize	By working together with private industry, the SSAs and State and local agencies can make sure that they are providing consistent information to DHS and all parties understand why some assets are viewed as more critical than others.	Coordinated requests for funding, both in terms of the assets covered and across agencies.
	When the parties do not coordinate, there is a greater chance funding will be misallocated. This may occur because too many things are labeled as critical or because the same asset gets funding from several sources unnecessarily.	
Implement Protective Measures	By working together to assess risks, determine opportunities for protective measures, and identify gaps in current measures, it will be easier to develop protective strategies tailored to each asset. The balance between government and private resources can be considered, particularly in terms of which types of measures each party is responsible for.	By working through the States and localities, funding can be targeted at regions rather than individual systems or facilities.
	By engaging industry and working with the State and local agencies improvements that benefit multiple sectors—whether it is in shared communication systems, better emergency response capabilities, or joint plans for backup capabilities can be made.	
Measure Effectiveness	Improved CI/KR protection should be measured locally as well as within sectors. State and local agencies and private industry can help the SSAs to define and track meaningful measures.	Demonstrating effectiveness may be a requirement for ongoing funding.

7.6 Key Implementation Actions

All milestones are specified with respect to the date of final signature of the NIPP. If agencies are not able to meet milestones they should notify the Secretary of Homeland Security in a letter specifying the reason and the date by which they will be able to achieve the milestone.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
7.1 Determining Sector Requirements								
DHS	Develop a set of annual CI/KR protection priorities based on the risk management framework to provide HSC and OMB a complete picture of CI/KR protection programs and resources.							X
SSA	Develop an annual list of sector priorities and resource needs, consistent with national policy, but focused on CI/KR protection needs by their sector.							X
7.2 Prioritizing by National Critical Asset								
DHS	Build cases for the designation of funds at the Federal level for CI/KR protection programs.							
DHS	Coordinate with Federal departments, agencies, OSLGCP, State and Territorial governments to ensure that CI/KR protection activities are adequately considered in the budget process.						X	
SSAs	Deliver prioritized list of sector assets to DHS Secretary.							X
DHS	Coordinate with OMB and HSC on the allocation of CI/KR protection resources, either through appropriated funds or the use of homeland security grants.							X
SSAs	Coordinate with DHS, HSC, and OMB to obtain funding through their budget process to maintain sector-level CI/KR protection programs.							X
7.3 Adjudicating Allocation of Federal Resources								
HSC	Provide a mechanism for annual interagency review by November 1.							
DHS OSTP	Work with OMB to identify, communicate, and advocate funding allocations supporting priority areas for CI/KR protection R&D in the appropriate agencies.							
HSC	Provide a synopsis to OMB for use in building the President's budget submission.							X
7.4 Grant Monies for CI/KR Protection								
DHS	Develop guidance for State, Territorial, and tribal CI/KR protection plans, aligned with requirements for grant applications.				X			
SSAs	Identify potential funding sources for sector CI/KR.							X

KEY: SP = Security Partners, DHS = Department of Homeland Security, SSAs = Sector-Specific Agencies, HSC = Homeland Security Council.

Glossary of Key Terms

All-Hazards. An approach to risk management that addresses the vulnerabilities, consequences, and threats posed by both natural and manmade events.

Annex. Separate sector-specific plans which have been incorporated under the NIPP for planning purposes.

Appendix. Supplemental material provided within this document to provide additional detail on activities, programs, and concepts within the NIPP.

Asset. As defined in the Homeland Security Act of 2002, assets include contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel). This Plan further defines an infrastructure asset as something of importance or value belonging to one of the 17 CI/KR sectors that if targeted and exploited, destroyed, or incapacitated could result in large-scale injury, death, economic damage, or destruction of property, or could profoundly damage the Nation's prestige and confidence.[14] Assets include one or more of the following elements:

- *Physical elements:* Tangible property such as facilities, components, real estate, animals, and products.
- *Cyber elements:* Electronic information and communications systems and the information contained in those systems, and comprising all the hardware and software that processes (i.e., creates, accesses, modifies, and destroys), stores (via all media types including paper, magnetic, and electronic), and communicates (i.e., shares and distributes) information, or any combination of all of these elements.[15]
- *Human or living elements:* Critical knowledge or functions of people (i.e., job expertise or skills) uniquely susceptible to attack.

Center of Excellence. A coordinated, university-based, system designed to establish and enhance the Nation's homeland security by means of research and education.

Consequence. The result of a terrorist attack on infrastructure assets reflecting the level, duration, and nature of the loss resulting from the attack. HSPD-7 notes three different types of consequence:

- *Exploitation:* The use of an infrastructure asset against some other target. Any evaluation of the consequences of the exploitation of an asset must consider whether the asset can be modified, influenced, changed, employed, leveraged, or commandeered in a manner that would enable attacks on other targets.[16]
- *Destruction:* The total loss of an infrastructure asset, function, or service; a permanent or long-term consequence. Destruction of an asset may also include collateral damage affecting related assets.
- *Incapacitation:* The partial loss of an infrastructure asset, function, or service; a short-term consequence from which recovery is possible.

HSPD-7 explains that terrorists seek to effect these three types of consequences in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence.

Credible Threat. A potential terrorist threat that, based on a threat assessment, is believable.

---

[14] *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (February 2003), page 7.

[15] Cyber is unique in that it does not necessarily function for itself; rather it is an enabler for a sector's critical functions and services. Cyber facilitates the business and operational aspects of a sector. A sector's functions and services are enhanced through secure cyber implementation.

[16] Some examples of exploitation are: the use of the Internet, business networks, or individual computers to attack infrastructure; the use of transportation systems to carry resources to facilitate an attack; or the use of people to gain information about an asset (social engineering).

Critical Infrastructure Information (CII). As defined by the Critical Infrastructure Information Act of 2002, CII includes information not customarily in the public domain and related to the security of critical infrastructure or protected systems involving:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, Territorial, tribal, or local law; harms interstate commerce in the United States, or threatens public health or safety;
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Critical Infrastructures/Key Resources. Systems, assets, or functions, whether physical or virtual, publicly or privately owned, that are used by or provide benefit to the public and are so vital to the U.S. that the exploitation, destruction, or incapacitation of such systems, assets, or functions would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Protection. The activities undertaken through the risk management framework that reduce risk for CI/KR assets or systems.

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and if needed the restoration of, electronic information and communications systems and the information contained therein; to ensure the information's confidentiality, integrity, and availability.

Dependency. The one-directional reliance of an asset, sector, or sectors on other input, interaction, or other requirement in order to function properly.

Government Coordinating Council (GCC). The government counterpart to the Sector Coordinating Council for each sector established to enable interagency coordination. The GCC is comprised of representatives across various levels of government (Federal, State, Territorial, tribal, and local) as appropriate to the security landscape of each individual sector.

Homeland Security Advisor. The chief designated official responsible for homeland security efforts in a particular State or Territory.

Incident of National Significance. Based on criteria established in HSPD-5 (paragraph 4), an actual or potential high-impact event that requires a coordinated and effective response by and appropriate combination of Federal, State, Territorial, tribal, local, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities.

Interdependency. The reliance of an asset, sector, or sectors on other assets or sectors to function properly, and their reliance on the original entity in return. This reliance is reciprocal and at a minimum, bidirectional.

Jurisdiction. A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or

geographic (e.g., city, county, tribal, State, Territorial, or Federal boundary lines) or functional (e.g., law enforcement, public health). (Source—NIMS, March 2004)

Local Government. Local means "(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity." (Source: Homeland Security Act of 2002)

National Special Security Event (NSSE). A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity.

Normalize. The process of transforming risk data into comparable units.

Preparedness. The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources.

Prevention. Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; immunizations, isolation, or quarantine; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Prioritize. The process of using risk assessment results to identify where risk-reduction efforts are most needed and subsequently determine which protective actions should be instituted first.

Protect and Secure. As defined in HSPD-7, reducing the threat, vulnerability, or consequences associated with attack on CI/KR assets, systems, or interconnecting links by deterring, mitigating, or neutralizing terrorist attacks.

Recovery. The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Region. An area with shared geography, economies, or other characteristics that encompasses distinct political entities that can serve as the focal point for infrastructure protection through partnerships of public and private security partners and sector interests.

Response. Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and

source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence.

Risk Management Framework. A planning methodology that outlines the process for setting security goals, identifying assets, assessing risks, prioritizing and implementing protective programs, and measuring effectiveness to produce a comprehensive, systematic, and rational assessment of national, or sector risk that drives CI/KR risk-reduction activities.

Sector. A logical collection of assets that provides a common function to economy, government, or society. The NIPP addresses 17 CI/KR sectors.

Sector Coordinating Council (SCC). Self-organized, self-run, and self-governed organizations that are fully representative of owners and operators within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of infrastructure protection activities and issues, including information sharing.

Sector Partnership Model. The framework for key security partners in the private sector, Federal agencies, States, Territories, local governments, and tribes to work together seamlessly in robust, public-private partnerships.

Sector-Specific Agency (SSA). Federal departments and agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors.

Sector-Specific Plan (SSP). Annexes to the NIPP Base Plan that detail the application of the NIPP core processes specific to each CI/KR sector. SSPs are developed by HSPD-7-designated SSAs in coordination with other security partners.

Security Partner. A Federal, State, Territorial, tribal, regional, or local government entity, private sector owners and operators of infrastructure, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

State Government. State means "any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States." (Source: Homeland Security Act of 2002)

Steady-State. In the context of the NIPP, the posture for routine normal day-to-day operations verses periods of heightened alert, or response to threats or incidents.

System. A collection of resources or elements made up of any combination of functions, physical attributes, or cyber components that perform a process. The elements of a system may be distributed and interconnected across the globe.

Terrorism. Any activity that (1) involves an act that is: (a) is dangerous to human life or potentially destructive of critical infrastructure or key resources, and (b) a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat. An indication of possible violence, harm, or danger.

Vulnerability. A weakness the design, implementation, or operation of an asset or system that can be exploited by an adversary or disrupted by a natural hazard.

Weapon of Mass Destruction (WMD). As defined in Title 18, U.S.C. § 2332a: (1) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

List of Acronyms and Abbreviations

ACAMS	Automated and Critical Asset Management System
ANSI	American National Standards Institute
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia Pacific Economic Cooperation
ACAMS	Automated Critical Asset Management System
BZPP	Buffer Zone Protection Program
CAEIAE	Centers of Academic Excellence in Information Assurance Education
CCIPS	Computer Crime and Intellectual Property Section
CFIUS	Committee on Foreign Investment in the United States
CII	Critical Infrastructure Information
CI/KR	Critical Infrastructure/Key Resources
CIP	Critical Infrastructure Protection
COI	Communities of Interest
CONOPS	Concept of Operations
COOP	Continuity of Operations Plans
COP	Common Operational Picture
CR	Comprehensive Review
CSIA IWG	Cybersecurity and Information Assurance Interagency Working Group
CSIRT	Computer Security Incident Response Teams
CSSC	Control Systems Security Center
CV	Characteristics and Common Vulnerabilities
CWIN	Critical Infrastructure Warning Information Network
Cyber NIE	Cyber National Intelligence Estimate
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
ECTF	Electronic Crime Task Force
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only

1	FPS	Federal Protective Service
2	GCC	Government Coordinating Council
3	GFIRST	Government Forum of Incident Response and Security Teams
4	GSA	General Services Administration
5	HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
6	HSA	Homeland Security Advisor
7	HSAC	Homeland Security Advisory Council
8	HSAS	Homeland Security Advisory System
9	HSC	Homeland Security Council
10	HSIM	Homeland Security Information Messages
11	HSIN	Homeland Security Information Network
12	HSIN-CI	HSIN-Critical Infrastructure
13	HSIN-CS	HSIN-Critical Sector
14	HSIN-CT	HSIN-Counter Terrorism
15	HSIN-EM	HSIN-Emergency Management
16	HSIN-LE	HSIN-Law Enforcement
17	HSOC	Homeland Security Operations Center
18	HSPD	Homeland Security Presidential Directive
19	HSSP	Homeland Security Standards Panel
20	IACC	Inter-Agency Coordination Cell
21	ICE	Immigration and Customs Enforcement
22	ID	Identification
23	IDWG	Internet Disruption Working Group
24	IIMG	Interagency Incident Management Group
25	IP	Infrastructure Protection (Division of DHS Preparedness Directorate)
26	ISAC	Information Sharing and Analysis Center
27	ISC	Interagency Security Committee
28	ISO	International Organization for Standards
29	IT	Information Technology
30	IWWN	International Watch and Warning Network
31	JHOC	Joint Harbor Operations Center
32	JRIES	Joint Regional Information Exchange System
33	LES	Law Enforcement Sensitive
34	LLE	Local Law Enforcement

1	MBA	Master of Business Administration
2	MS-ISAC	Multi-State Information Sharing and Analysis Center
3	NADB	National Asset Database
4	NATO	North Atlantic Treaty Organization
5	NCC	National Coordinating Center [for Telecommunications]
6	NCIP R&D	National Critical Infrastructure Protection Research and Development
7	NCR	National Capital Region
8	NCRCG	National Cyber Response Coordination Group
9	NCSA	National Cybersecurity Alliance
10	NCSD	National Cybersecurity Division
11	NIAC	National Infrastructure Advisory Council
12	NICC	National Infrastructure Coordinating Center
13	NIH	National Institutes of Health
14	NIMS	National Incident Management System
15	NIPP	National Infrastructure Protection Plan
16	NISAC	National Infrastructure Simulation and Analysis Center
17	NIST	National Institute of Standards and Technology
18	NITRD	Networking and Information Technology Research and Development
19	NOAA	National Oceanic and Atmospheric Agency
20	NRC	Nuclear Regulatory Commission
21	NRP	National Response Plan
22	NSA	National Security Agency
23	NS/EP	National Security/Emergency Preparedness
24	NSF	National Science Foundation
25	NSSE	National Security Special Event
26	NSTAC	National Security Telecommunications Advisory Committee
27	NSTC	National Science and Technology Council
28	OAS	Organization of American States
29	OECD	Organization for Economic Cooperation and Development
30	OIC	Office for Interoperability
31	OMB	Office of Management and Budget
32	OPM	Office of Personnel Management
33	OSLGCP	Office for State and Local Government Coordination and Preparedness
34	OSTP	Office of Science and Technology Policy

1	PCII	Protected Critical Infrastructure Information
2	PCS	Process Control System
3	PDD	Presidential Decision Directive
4	PI	Potential Indicators of Terrorist Activity Report
5	PITAC	President's Information Technology Advisory Committee
6	PKI	Public Key Infrastructure
7	PM	Protective Measure Report
8	PNWER	Pacific NorthWest Economic Region
9	PSA	Protective Security Advisor
10	PVTSAC	Private Sector Senior Advisory Committee
11	RAMCAP	Risk Analysis and Management for Critical Asset Protection
12	R&D	Research and Development
13	SAA	State Administrative Agency
14	SCADA	Supervisory Control and Data Acquisition
15	SCC	Sector Coordinating Council
16	SCEPC	Senior Civil Emergency Planning Committee
17	SFS	Scholarship for Service
18	SOP	Standard Operating Procedure
19	SP	Security Partner
20	SPP	Security and Prosperity Partnership of North America
21	SSA	Sector-Specific Agency
22	SSP	Sector-Specific Plan
23	S&T	Science and Technology Directorate of DHS
24	SVA	Security Vulnerability Assessment
25	TSA	Transportation Security Administration
26	UASI	Urban Areas Security Initiative
27	U.K.	United Kingdom
28	U.S.	United States
29	U.S.-CERT	United States Computer Emergency Readiness Team
30	USCG	United States Coast Guard
31	USSS	United States Secret Service
32	ViSAT	Vulnerability Identification Self-Assessment Tool
33	VRPP	Vulnerability-Reduction Purchasing Plan
34	WMD	Weapons of Mass Destruction

Appendices

Appendix A: Cross-Sector Cyber Element

Foreword

This appendix provides additional details on processes, procedures, and mechanisms needed to achieve NIPP goals and the supporting objectives for cybersecurity. It specifies cyber responsibilities for security partners, processes and initiatives to reduce risk and milestones and metrics to measure progress in achieving the plan's overarching goal that will be used to enhance the Nation's protection of cyber infrastructure.

It is focused on *consumers* of cyber infrastructure, including CI/KR sectors and their associated security partners. The producers of cyber infrastructure (i.e., the IT industrial base) are addressed in the information technology (IT) sector-specific plan (SSP). It is organized to be aligned with the chapters of the NIPP to provide the reader with context for the additional information as follows:

A.1 Introduction

A.2 Cyber Responsibilities

A.3 Managing Cyber Risk

A.4 Ensuring Long-Term Cybersecurity

A.1 Introduction

The U.S. economy and national security are fully dependent upon the cyber infrastructure. Cyber infrastructure enables the Nation's essential services, resulting in a highly interconnected and interdependent network of CI/KR. This network enables services such as the Internet and financial markets, and also controls many critical processes, including the electric power grid, and chemical processing plants.

A spectrum of malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. Of primary concern is the risk of organized cyber attacks capable of causing debilitating disruption to the Nation's CI/KR, economy, or national security. Furthermore, while terrorist groups have not yet launched a debilitating attack against the Internet, there is ample evidence of their use of this medium as a means of attack or for other purposes. In addition, the increasing ease with which powerful cyber attack tools can be obtained and used places the ability to conduct cyber attacks within reach of most groups or individuals wishing to do harm to the United States.

Sectors' functions and services are enabled through IT systems and services; however, if cybersecurity is not integrated appropriately, the risk to sectors' missions is greatly increased.

DHS has developed the following cybersecurity vision:

> *DHS is committed to securing cyberspace by working collaboratively with public, private, academic, and international entities to ensure that the owners and operators of the critical infrastructure are knowledgeable and adequately prepared to foresee and, if possible, prevent cyber attacks; and that the cyber elements of the critical infrastructure are:*
>
> - *Robust enough to withstand attacks without incurring catastrophic damage;*
> - *Responsive enough to recover from attacks in a timely manner; and*
> - *Resilient enough to sustain nationally critical operations.*

A.1.1 Definitions

The following definitions provide additional explanation to answer the question "What is cyber?" in the context of CI/KR protection:

- **Cyber infrastructure:** Includes electronic information and communications systems and the information contained in those systems. Information and communications systems are comprised of all the hardware and software that processes (i.e., creates, accesses, modifies, and destroys), stores (e.g., all media types: paper, magnetic, and electronic), and communicates (i.e., shares and distributes) information, or any combination of all of these elements. For example, computer systems and networks, such as the Internet, are part of cyber infrastructure.
    - "Producers" of cyber infrastructure are the IT industrial base, which comprise the IT Sector.
    - "Consumers" of cyber infrastructure must maintain its security in a changing threat environment. Individuals, whether private citizens or employees with cyber systems administration responsibility, play a significant role in managing the security of computer systems to ensure that they are not used to enable attacks against CI/KR.
- **Cybersecurity:** The prevention of damage to, unauthorized use of, exploitation of, and the restoration of electronic information and communications systems and the information contained therein; to ensure the information confidentiality, integrity, and availability.
- **Cross-sector cyber:** Collaborative efforts between DHS and SSAs to ensure that deployed cyber elements have been secured in an appropriate and consistent manner across sectors.

A.1.2 Cyber-Specific Authorities

Various Federal strategies, directives, policies, and regulation provide the basis for Federal actions and activities associated with implementing the cyber-specific aspects of the NIPP. The two primary authorities associated with cybersecurity are the *National Strategy to Secure Cyberspace* and HSPD-7. These documents are described in further details in Section 1.6 of the NIPP.

A.2 Cyber Responsibilities

According to the National Strategy to Secure Cyberspace and HSPD-7, security partners have significant roles and responsibilities in the security of cyberspace. These roles and responsibilities are described in more detail below.

A.2.1 Department of Homeland Security

DHS is a focal point for the security of cyberspace. DHS has specific responsibilities regarding the coordination of the efforts of security partners to prevent damage to, unauthorized use, exploitation, and enable the restoration of electronic information and communications systems and the information contained therein to ensure information confidentiality, integrity, and availability. These responsibilities include:

- Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems;
- Coordinating with other agencies of the Federal Government to provide specific warning information and advice about appropriate protective measures and countermeasures to State, Territorial, local, and nongovernmental organizations including the private sector, academia, and the public;

- Performing and funding R&D along with other agencies that will lead to new scientific understanding and technologies in support of homeland security; and
- Assisting SSAs in understanding and mitigating cyber risk and in developing effective and appropriate protective measures.

Within the risk management framework described in the NIPP, DHS is also responsible for the following activities:

- Providing cyber-specific expertise and assistance in addressing the cyber elements of CI/KR;
- Promoting a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own segments of cyberspace;
- Working with security partners to reduce cyber vulnerabilities and minimize the severity of cyber attacks;
- Leading in the development and conduct of a national cyber threat assessment;
- Facilitating cross-sector cyber analysis to understand and mitigate cyber risk;
- Providing guidance, review, and functional cyber advice on the development of effective and appropriate protective measures; and
- Coordinating cybersecurity protective programs and contingency plans, including a plan for recovering Internet functions.

A.2.2 Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics and operating models, SSAs provide the subject matter and industry expertise through relationships with the private sector to ensure protection of the assets within their sectors. SSAs must understand and mitigate cyber risk by developing effective and appropriate protective measures for cyber assets and systems in their respective sectors:

- Identifying subject matter expertise within their sector to address the unique cyber aspects;
- Increasing awareness of how the business and operational aspects of the sector relies on cyber systems and processes;
- Determining if approaches for asset identification, risk assessment, and protective measures, currently address cyber assets and systems, require enhancement, or require use of alternative approaches;
- Reviewing and updating existing and future sector efforts to ensure that cyber concerns are fully integrated;
- Establishing mutual assistance programs for cybersecurity emergencies; and
- Exchanging cyber-specific information with sector security partners, including the international community, as appropriate to improve the Nation's overall cybersecurity posture.

A.2.3 Other Federal Departments and Agencies

All Federal departments and agencies must manage the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR. However, a number of other Federal agencies have specific responsibilities outlined in the *National Strategy to Secure Cyberspace*:

- **The Department of Justice and the Federal Trade Commission:** Working with sectors to address barriers to mutual assistance programs for cybersecurity emergencies.

- **The Department of Justice and other Federal Agencies**:
  - Developing and implementing efforts to reduce cyber attacks and cyber threats through developing better data about victims of cyber crime and intrusions in order to understand the scope of the problem and be able to track changes over time;
  - Exploring means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of CI/KR incidents; and
  - Identifying ways to improve information sharing and investigative coordination within the Federal, State, Territorial, and local law enforcement community working on CI/KR and cyberspace security matters, and with other agencies and the private sector.
- **The Federal Bureau of Investigation and Intelligence Community:** Ensuring a strong counterintelligence posture to counter cyber-based intelligence collection against the U.S. Government, and commercial and educational organizations.
- **The Intelligence Community, the Department of Defense, and the Law Enforcement Agencies:** Improving the nation's ability to quickly attribute the source of threatening attacks or actions to enable timely and effective response; efforts will seek to develop capabilities to prevent attacks from reaching CI/KR.

A.2.4 State, Territorial, Tribal, and Local Governments

State, Territorial, tribal, and local governments have the following cyber responsibilities:

- Managing the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR; and
- Establishing IT security programs, including awareness, audits, and standards.

A.2.5 Private Sector

The private sector has a number of responsibilities outlined in the *National Strategy to Secure Cyberspace* that include:

- Managing the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR;
- Reviewing and exercising IT continuity plans and considering diversity in IT service providers as a way of mitigating risk;
- Considering active involvement in industry-wide programs to share information on cybersecurity;
- Considering including in near-term R&D priorities, programs for highly secure and trustworthy operating systems. If such systems are developed and successfully evaluated, the Federal Government will, subject to budget considerations, accelerate procurement of such systems;
- Evaluating the security of networks that impact the security of the Nation's CI/KR which may include: conducting audits to ensure effectiveness and use of best practices, developing continuity plans that consider offsite staff and equipment, and participating in industry-wide information sharing and best practice dissemination; and
- Promoting more secure "out of the box" installation and implementation of software industry products including increasing user awareness of the security features in products; ease of use for

security functions; and where feasible, promotion of industry guidelines and best practices that support such efforts.

A.2.6 Academia

Colleges and universities have several specific responsibilities outlined in the *National Strategy to Secure Cyberspace*:

- Managing the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that computer systems are not used to enable attacks against the Nation's CI/KR;
- Considering establishing one or more information-sharing mechanisms to deal with cyber attacks and vulnerabilities, and an on-call point of contact to Internet service providers and law enforcement officials in the event that the school's cyber assets or systems are discovered to be launching cyber attacks; and
- Securing cyber systems by establishing some or all of the following as appropriate—one or more information-sharing mechanisms to deal with cyber attacks and vulnerabilities, model guidelines empowering Chief Information Officers to address cybersecurity, one or more sets of best practices for IT security, and model user awareness programs.

A.3 Managing Cyber Risk

A.3.1 Set Security Goals

The goals and objectives set forth in the NIPP provide the overarching direction for the CI/KR protection effort. Since cyber concerns are not unique to any one sector, successful cyber CI/KR protection efforts across all sectors require close collaboration by security partners. This involves taking actions to achieve five programmatic objectives that define an additional level of detail to guide cyber-focused CI/KR protection efforts. The following sections provide a brief discussion of each objective, its benefits, and indicate the location(s) in this cyber appendix that describe the initiatives, milestones, and processes to achieve the desired outcomes.

Objective 1: Establish a National Cyberspace Security Response System

Establishing a National Cyberspace Security Response System to prevent, detect, respond to, and reconstitute rapidly after a cyber incident will help to:

- Increase dissemination, awareness, and analysis of threats and responses to build and improve situational awareness capabilities;
- Promote collaboration, coordination, and information sharing among public, private, and international communities;
- Create and pursue an international cyber strategy to secure cyberspace;
- Protect government cyberspace; and
- Improve the Nation's cybersecurity readiness, protection, and incident response capabilities by creating, sponsoring, and learning from national, regional, and interagency exercises and workshops.

Section A.3.5 of this appendix describes cybersecurity initiatives for the government and exercises to practice effective collaborative response to cyber attack. Section A.4 of this appendix describes information sharing and international efforts to improve collaboration and coordination.

Objective 2: Reduce Vulnerabilities and Minimize the Severity of Cyber Attacks

Working with the public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks will help improve the cybersecurity of CI/KR, including the promotion of cybersecurity by reducing risks to control systems and improving the security of software across the development life cycle. Section A.3.3 of this appendix describes efforts to promote cybersecurity and reduce vulnerabilities of the cyber infrastructure, including software and control systems.

Objective 3: Promote a National Awareness Program

An important objective is to promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own segments of cyberspace. This will help the cyber CI/KR protection efforts by:

- Building and maintaining trusted relationships with industry, government, and academia to raise cybersecurity awareness and foster collaborative efforts to secure cyberspace; and
- Establishing a national cybersecurity outreach and awareness program to manage outreach, cybersecurity awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key security partners.

Section A.4 of this appendix describes outreach and awareness initiatives to empower security partners to secure cyberspace.

Objective 4: Foster Cyber Training and Education Programs

Training and education is an important component of establishing a knowledge base for the security of cyberspace. To attain the objective of fostering adequate training and education programs to support the Nation's cybersecurity needs, the development of cybersecurity professionals via training and education programs is needed. Section A.4 of this appendix describes training and education programs to help develop cybersecurity professionals.

Objective 5: Identify and Reduce Threats to Cyberspace

Because of the nature of cyberspace, threats can emerge from anywhere at anytime. Unlike physical based threats, cyber threats can be more difficult to identify and track. DHS will identify and reduce threats to cyberspace by:

- Improving a coordinated cyber intelligence capability; and
- Improving threat detection and deterrence capabilities.

Section A.3.5 and Section A.4 of this appendix describe efforts to reduce threats to cyberspace through improved interagency coordination.

A.3.2 Identify Cyber Assets

During NIPP risk analysis, cyber assets and systems are examined both as individual entities and as one of three elements (along with human and physical) of a larger function, product, or service that should be identified. The process for identifying cyber assets or systems should be repeatable, scalable, and distributable, enabling cyber dependency analysis at both the sector and national and levels in order to prioritize risk mitigation techniques.

Cyber assets represent a variety of hardware and software components. Examples include networking equipment, database servers, security systems, operating systems, and database software. Cyber systems are a set of cyber assets that interact to perform a particular function. The following is a list of cyber assets or systems that exist in most, if not all, sectors that should be identified individually or included as a cyber element of a physical asset's description if they are associated with one:

- **Automated access control** is a process that is common to all sectors supporting physical access control (has cyber, as well as human and physical, elements). The human and physical elements are commonly recognized, such as people possessing access cards and scanners outside of the facility. However, the cyber elements are less easily recognized because they are typically behind the scenes. They are the hardware and software that process, store, and communicate electronic information. For example, there may be database servers that store individuals' names and software that process access attempts.

- A **control system** is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Various types of control systems are used within many sectors in different ways. Examples include the management of the electric power grid using supervisory control and data acquisition (SCADA) systems within the energy sector and process control systems (PCS) that control the timing and volume of chemical processes within the chemical sector. Control systems generally consist of two parts: (1) operator interfaces (also known as human-machine interfaces), and (2) field controllers. Both are computer-based. These systems are particularly problematic because their life cycle is typically 15+ years, in contrast to the 12 to18-month life cycle of business cyber systems. Typical cybersecurity measures do not often work in this operations-oriented environment. Such control systems were designed for specific uses in isolation, but have become connected to the business networks and are thus vulnerable to the latest attack vectors.

Based on the definitions in this NIPP, the critical elements of the **Internet** are considered CI/KR. The Internet is composed of assets within both the IT and Telecommunications Sectors and used by all sectors in varying degrees of business and operational dependence, and which extend beyond the Nation's borders into international cyberspace. While the availability of the Internet is the responsibility of the IT and Telecommunications Sectors, the need for access to and reliance on the Internet is common to all sectors.

DHS is developing a cross-sector cyber asset identification methodology that, when applied, would enable a sector to identify cyber entities and characterize the reliance of a sector's business and operational functionality on cyber. The draft methodology includes determining nationally consequential functions, products, and services using of HSPD-7 consequences, developing a sector model, and applying a cyber dependency filter to identify cyber assets or systems. Additional documentation on this methodology will be available from DHS in the second quarter of FY2006. If a sector's cyber asset identification methodology already exists, the sector needs to partner with DHS to ensure alignment of that methodology with the NIPP risk management framework described in Chapter 3 of the NIPP.

Divisions within DHS are collaborating on the National Asset Database (NADB) effort to incorporate common cyber categories across all sectors into each individual sector's taxonomy. This effort is a work-in-progress, however, the intent is that the taxonomy will encourage and enable the identification of common cyber assets and those that may be unique to the sector.

A.3.3 Assess Risks

The risk assessment for cyber assets and systems is an integral part of the NIPP risk management framework described in the NIPP. The NIPP risk management framework combines consequences, threats, and vulnerabilities to produce systematic, comprehensive, and defensible risk assessments. DHS and the SSAs will assess risk for cyber assets and inputs supplied by all levels of CI/KR security partners.

DHS will incorporate the results of this risk assessment in its overall risk management process to prioritize where the Nation's limited resources for CIP activities will be applied.

A.3.3.1 Consequence Analysis

The first step in the risk assessment process is the determination of the consequences of destruction, incapacitation, or exploitation of an asset. HSPD-7 identifies six nationally significant consequence categories, that are listed in Section 3.3.1of the NIPP.

To assess whether a given asset may be nationally consequential, physical, human, and cyber asset **dependencies and interdependencies** need to be assessed. Cyber interdependence presents a unique challenge for all sectors because the cyber infrastructure often enables sectors' critical services and the borderless nature of cyberspace. Cyber interdependence is characterized by a sector's reliance on hardware and/or software that processes, stores, or communicates electronic information, and cyber's reliance on the infrastructure. Interdependencies are dual in nature—for example, the energy sector's reliance on computer-based control systems to manage the electric power grid, while those same control systems require power to operate.

Sophisticated modeling and simulations through the National Infrastructure Simulation and Analysis Center (NISAC) will quantify national and international dependency and interdependency and their impacts. However, this effort is complex and time consuming. In the interim, dependency and interdependency analysis must be done in a qualitative manner with the participation of subject matter experts within and across sectors. These qualitative assessments are an important and more immediate component of overall dependency and interdependency analyses. For cyber dependency and interdependency analyses, sectors should identify subject matter experts within their sector who are knowledgeable about the cyber aspects of their sector and include that expert qualitative assessment when assessing assets' consequences.

The **consequences** of the destruction, incapacitation, or exploitation of assets must be measured and described in terms of the national risk scale to determine if they are nationally consequential. The national risk scale provides a common basis for comparing risk and allows consequences to be quantified on the basis of impact to health, economic, psychological, national security, or government function. DHS is developing and refining this risk scale as part of the Risk Analysis and Management for Critical Asset Protection (RAMCAP) framework.

While the RAMCAP process and the national risk scale apply equally to both physical and cyber risks, it is essential to properly account for cyber assets and vulnerabilities since these are often underrepresented. For example, a well-executed cyber attack on the Nation's financial systems could diminish consumer confidence and have massive, long-term economic impacts.

A.3.3.2 Vulnerability Assessment

The second step of the risk process is analysis of vulnerability—determining which elements of infrastructure are most susceptible to attack and how attacks against these elements would be carried out. DHS is working to identify cross-sector best practices to ensure that SSA's existing methodologies address cyber vulnerabilities and has taken a broad, inclusive approach by reviewing various existing publicly available methods across industry, government, and academia, to assemble a hybrid of the best practices. For example, DHS is not only examining many of the very detailed vulnerability standards from the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST), but is also looking at higher level vulnerability assessment methods in use within the law enforcement/intelligence community. DHS is also working to leverage well-established methodologies that have traditionally focused on physical vulnerabilities, by enhancing them to better address cyber elements. Examples of these efforts include the enrichment of DHS' Vulnerability Identification Self Assessment Tool (ViSAT), as well as the RAMCAP process. The hybrid set of cross-sector vulnerability assessment best practices will be available beginning in the second quarter of FY2006.

There are cyber vulnerabilities that all sectors should consider when conducting their assessments, such as system interconnections. System interconnections (also known as trusted connections) are defined as the direct connection of two or more IT systems owned by separate organizations. Business or government offices may interconnect for a variety of reasons, depending on the relationship between the interconnected entities. Unfortunately, system interconnections may increase the security risk by exposing one system to vulnerabilities associated with another location. This risk is exacerbated because most organizations do not have control over the operation and management of their business partner's IT systems.

DHS has established several vulnerability-reduction programs under the CIP risk management framework, including: the Software Assurance Program and the U.S.-CERT Control Systems Security Center (CSSC).

A.3.3.2.1 Software Assurance

DHS is working to develop best practices and new technologies to promote integrity, security, and reliability in software development. DHS is leading the Software Assurance Program, a comprehensive software assurance strategy that addresses people, process, technology, and acquisition throughout the software development lifecycle. DHS' efforts to achieve a broader ability to routinely develop and deploy trustworthy software products and ensure the continued competitiveness of the U.S. software industry through public-private partnerships are a significant element of securing cyberspace and the Nation's critical infrastructure. These efforts will lead to the production of higher quality, more secure software. The overall goal is secure and reliable software supporting mission requirements, enabling more resilient organizations.

The Software Assurance Program is designed to lead the development of practical guidance and review tools, and promote R&D investment in cybersecurity. As part of its efforts, DHS co-sponsors the National Vulnerability Database (NVD), a set of centralized and comprehensive vulnerability information in order to assist with incident prevention and management (including patches) to mitigate the impact of vulnerabilities. Additionally, the program is conducting a comprehensive review of the National Information Assurance Partnership (NIAP) to determine the extent to which it adequately addresses security flaws. The NIAP promotes the development of sound security requirements for IT products and systems, as well as appropriate security evaluation metrics.

A.3.3.2.2 Control System Security

A control system is an interconnection of components (designed to maintain operation of a process or system) connected or related in such a manner as to command, monitor, direct, or regulate itself or another system. Control systems are embedded throughout the Nation's CI/KR (e.g., chemical, manufacturing, water treatment, and food processing plants, transportation systems, oil and gas refineries, power generation plants, and transmission systems). They are implemented with remote access and open connectivity, which exposes them to increasing cyber threats that could have a devastating impact on national security, economic security, and public health and safety, as well as the environment. DHS' Control Systems Security Initiative coordinates efforts among Federal, State, Territorial, tribal, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. DHS is leading a comprehensive national initiative to implement near term protection of control systems through the production and timely dissemination of situational awareness information to convey the "state of security" of the Nation's critical control systems. In August 2004, DHS created the U.S.-CERT Control Systems Security Center CSSC that develops and implements programs aimed at reducing the likelihood of success and the severity of impact of a cyber attack against critical infrastructure control systems. It coordinates government and industry activities to identify and mitigate control systems vulnerabilities, perform vulnerability assessments, and provide a national response capability for control systems incidents.

A.3.3.3 Threat Analysis

The third step of the risk assessment process is the analysis of threat, which provides the likelihood that a target will be attacked. There are increasing indicators that potential adversaries intend to conduct cyber attacks and are actively acquiring cyber attack capabilities. However, credible information on specific adversaries is frequently not available. Additionally, the increasing ease with which powerful cyber attack tools can be obtained and used places the ability to conduct cyber attacks within reach of most groups or individuals wishing to do harm to the United States. Therefore, DHS is collaborating with the intelligence and law enforcement communities and the private sector to more accurately portray the entire spectrum of cyber threat, including the use of the Internet as an attack vector (e.g., weapon).

As called for in the *National Strategy to Secure Cyberspace*, in late 2003 and early 2004, DHS provided input on cyber-related issues for the "National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure" (Cyber NIE). The Cyber NIE will be updated in this next year. Documents such as the Cyber NIE inform the threat scenarios in the General Threat Environment described in the NIPP.

A.3.4 Prioritize

DHS supports prioritization efforts to determine the most cost-effective ways to mitigate the Nation's highest risks. It is important that prioritization work include efforts to highlight cyber-related risks since attacks on any sector—either on or using that sector's cyber infrastructure—can have a devastating impact.

A.3.5 Implement Protective Programs

DHS recognizes that each sector will have a unique reliance on cyber infrastructure and, therefore, will assist the SSAs in developing a range of effective and appropriate cyber protective measures. In addition to individual sectors' protective measures, DHS has specific programs to help build a national cyberspace security response system:

- **Internet Disruption Working Group:** DHS coordinates cybersecurity contingency plans, including a plan for recovering Internet functions. To meet this mandate, DHS formed a strategic partnership in the Internet Disruption Working Group (IDWG) in January 2005 to combine resources, avoid duplication of effort, and leverage past Federal Government, academic, and private sector work. The working group will assess the operational dependency of critical infrastructure sectors on the Internet, and work with major security partners to identify and prioritize the short-term protective measures necessary to prevent major disruptions of the Internet or reduce their consequences and to identify responsive/reconstitution measures for contingency plans in the event of a major disruption. The IDWG will also work to assess the likelihood of a disruption within the operationally dependent sectors, and determine where vulnerability assessments are most needed. This group has also reviewed previous Internet disruption reports to identify high-priority actions to quickly and effectively improve the resiliency of the Internet.

- **National Cyber Exercises:** DHS is conducting exercises to identify, test, and improve coordination of the cyber incident response community, to include Federal, State, Territorial, tribal, local, and international government elements as well as private sector corporations and coordinating councils. The most comprehensive of these exercises is the National Cyber Exercise: Cyber Storm 2005. The main objectives of Cyber Storm 2005 are to practice effective collaborative response to a variety of cyber attack scenarios, including crisis decisionmaking; provide an environment for evaluation of interagency and inter-sector business processes reliant on the information infrastructure; measure the progress of ongoing U.S. efforts to defend against and respond to attacks; and foster improved information sharing among government agencies and between government and private industry. The Cyber Storm 2005 exercise will also sensitize a diverse constituency of private and public-sector

decisionmakers to a variety of potential cyber threats, including strategic attacks; familiarize this constituency with DHS' concept of a national cyber response system and the importance of their role in it; and practice roles and responsibilities of government agencies and industry in cyber incident response. Weaknesses discovered in government-wide processes during exercises will be included in agency corrective action plans and will be submitted to OMB.

- **The National Cyber Response Coordination Group:** The National Cyber Response Coordination Group (NCRCG) facilitates coordination of the Federal Government's efforts to prepare for, respond to and recover from cyber Incidents of National Significance and other national cyber incidents and physical attacks that have significant cyber consequences (hereinafter collectively "Cyber Incidents"). It serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber crisis. During such incidents, NCRCG member-agencies integrate their capabilities to assess the domestic and international scope and severity of a Cyber Incident. The NCRCG member-agencies use their situational awareness of a cyber incident to govern response and remediation efforts and to guide senior policymakers. NCRCG member-agencies also develop, coordinate, and recommend courses of action and incident response strategies for the U.S. Government. Moreover, NCRCG member-agencies use their established relationships with the private sector and State and local governments to help manage a cyber crisis, develop courses of action, and devise response and recovery strategies.

- **Programs for Federal Systems' Cybersecurity:** Federal agencies' prevention and protection efforts include those that are focused on securing their own cyber infrastructure. According to paragraph 34 of HSPD-7, "the heads of all Federal departments and agencies shall develop and submit to the Director of the Office of Management and Budget (OMB) for approval plans for protecting the physical and cyber CI/KR that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities." To assist Federal agencies in their efforts, DHS is acting as subject matter expert to OMB in reviewing the cyber aspects of Federal agency CIP plans to ensure that cyber risk is addressed consistently across all Federal agencies. DHS is also working with the OMB to improve Federal civilian agencies' cybersecurity posture and compliance with the Federal Information Security Management Act (FISMA).

- **Government Forum of Incident Response and Security Teams (GFIRST) :** DHS established the GFIRS to facilitate interagency information sharing and cooperation across Federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. The members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices.

Other examples of Federal agencies' cybersecurity access control, certification, and policy enforcement tools include:

- **The General Services Administration (GSA)** is responsible for developing and implementing a government-wide infrastructure for authentication services. In March 2004, GSA began to develop an automated risk assessment tool for government-wide use in certifying and accrediting its E-Authentication gateway. In addition, GSA is creating a list of approved solution providers that supply smart cards based on Federal Public Key Infrastructure (PKI) standards and that include a new electronic-authentication policy specification.

- **The National Oceanic and Atmospheric Agency (NOAA)** has implemented enterprise-wide vulnerability assessments, an intrusion detection system, enterprise wide virus detection software to enforce security policy, E500 virus scanning gateways, and a patch management policy.

A.3.6 Measure Effectiveness

There are several critical infrastructure core cyber measures and metrics that will be tracked across each sector to enable comparison and analysis between and among different types of critical infrastructure. The cyber core measures and metrics will mirror the core metrics and measures being developed for the NIPP, but will also include the review and consideration/ integration of common cybersecurity standards. Although those core metrics are still being developed, a sample of how these metrics and measures will be customized for cyber assets and systems are provided below in table A3-1.

Table A3-1: Sample Cyber Measures and Metrics

Cyber Measure	Description
1. Total number of cyber assets and systems	This descriptive cyber data will be collected for each Sector.
2. Number of cyber assets and systems with potential for medium or high consequences.	Tracking this measure will help determine which sectors are in the most need of assessing cyber vulnerabilities and if there are particularly critical regions or industries. This measure could be an outcome if protective actions intend to "devalue" assets to reduce potential consequences if they are compromised.
3. Percentage of medium or high consequence cyber assets and systems with completed vulnerability analyses.	Tracking this measure will help determine progress in determining which infrastructure assets and sectors are in the most need of protective and preventative programs.
4. Percentage of medium or high-consequence cyber assets and systems assessed as high risk.	Tracking this will help in determining which sectors require programs to increase preventive, protective, response and recovery capabilities. In conjunction with other measures and data on location and ownership of the assets, it can help focus government and private resources on those sectors, regions, and industries with the highest identified risks first.
5. Percentage of medium or high-consequence cyber assets and systems that have active protective programs to measurably reduce risk.	Tracking this, in conjunction with other measures, will help determine where there are potential gaps in program coverage for critical infrastructure cyber assets determined to be high risk.
6. Percentage of medium or high-consequence cyber assets and systems that have been assessed for readiness, response, and recovery capability.	Tracking this measure will provide insight into the effectiveness for cyber readiness, response, and recovery.
7. Percentage of cyber assets and systems reduced from high risk.	Tracking this measure will provide insight into the effectiveness of the programs implemented to reduce risk. Programs will reduce risk through a variety of means. For example, programs can reduce risk through creating a better response and recovery capability for the asset or increasing the difficulty of attacking critical infrastructure assets, or decreasing the probability of success of an attack against the asset via a variety of prevention and/or protective measures.

Once the core metrics have been developed and approved, a data gathering and reporting process will be established, in order to identify the necessary individuals and information for measuring progress. As

each sector's available data can differ, this process will have to take into consideration any unique situations that may arise. This process will outline, but will not be limited to, the responsible parties, data collection and reporting methodology, and timeframes for data and metrics submissions. Additionally, as the process matures, additional metrics will be considered to reflect the most important issues currently being faced by the sectors.

A.4 Ensuring Long-Term Cybersecurity

The effort to ensure a coherent cyber CI/KR protection program over the long term has four components which are described in greater detail below:

- **Information Sharing and Awareness** to ensure implementation of effective, coordinated and integrated CI/KR protection efforts of cyber assets and systems and enable cybersecurity partners to make informed decisions with regard to short- and long-term cybersecurity postures, risk mitigation, and operational continuity.
- **International Cooperation** to promote a global culture of cybersecurity and improve overall cyber incident preparedness and response posture.
- **Education and Training** to ensure that skilled and knowledgeable cybersecurity professionals are available to undertake NIPP programs in the future.
- **Research and Development** to improve cybersecurity protective capabilities or to dramatically lower the costs of existing capabilities so that State, Territorial, tribal, local, and private sector security partners can afford to do more with their limited budgets.

A.4.1 Information Sharing and Awareness

A.4.1.1 Interagency Coordination

Interagency cooperation and information sharing are essential to improving national cyber counterintelligence and law enforcement capabilities. The intelligence and law enforcement communities have various official and unofficial mechanisms in place for communication that DHS supports:

- **U.S. Secret Service's Electronic Crime Task Forces (ECTFs)** provide interagency coordination on cyber-based attacks and intrusions.
- **FBI's Inter-Agency Coordination Cell (IACC)** is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
- **FBI's InfraGard** program is a public-private partnership coordinated out of the 56 FBI field offices. The program brings together law enforcement, academia, and private sector entities on a monthly basis to provide a forum for information sharing and networking.
- **DOJ's Computer Crime and Intellectual Property Section (CCIPS**), the FBI, and the Secret Service meet regularly to coordinate and deconflict investigations, ensuring that there is no duplication of effort.
- **Cybercop Portal** is a secure Internet-based information-sharing mechanism for more than 5,300 law enforcement members involved in the field of electronic crimes investigations. The law enforcement community, including investigators from private industry (e.g., banks and the network security community), is tied together and supported by this secure, Internet-based, collaboration portal.

A.4.1.2 Cybersecurity Awareness for Security Partners

DHS has a leadership role in coordinating a public-private partnership to promote and raise cybersecurity awareness among the general public through:

- Partnering with other Federal and private sector organizations, to sponsor the National Cybersecurity Alliance (NCSA);
- Creating a public-private organization, Stay Safe Online, to educate home users, small businesses, and K-12 and higher education audiences on cybersecurity best practices; and
- Collaborating with the public and private sector to establish October as the National Cybersecurity Awareness Month and participated in activities to raise awareness of cybersecurity Nationwide.

A.4.1.3 Cyberspace Emergency Readiness

DHS established the **U.S. Computer Emergency Readiness Team (U.S.-CERT)** which is a 24/7 single point of contact for cyberspace analysis warning, information sharing, and incident response and recovery for a broad range of users, including government, enterprise, small businesses, and home users. U.S.-CERT is a partnership between DHS and the public and private sectors designed to protect the Nation's Internet infrastructure and to coordinate defense against and responses to cyber attacks across the Nation. U.S.-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating cyber incident response activities.

To support the information-sharing requirements of the networked approach, U.S.-CERT provides the following information on their Web site, accessible via the Homeland Security Information Network (HSIN), and via mailing lists:

- **Cybersecurity Bulletins:** Bulletins summarize information that has been published about new security issues and vulnerabilities. They are published weekly and are written primarily for system administrators and other technical users.
- **Technical Cybersecurity Alerts:** Written for system administrators and experienced users, technical alerts provide timely information about current security issues, vulnerabilities, and exploits.
- **Cybersecurity Alerts:** Written in language for home, corporate, and new users, these alerts are published in conjunction with technical alerts when there are security issues that affect the general public.
- **Cybersecurity Tips:** Tips provide information and advice about a variety of common security topics. They are published biweekly and are written primarily for home, corporate, and new users.
- **National Web Cast Initiative:** In an effort to increase cybersecurity awareness and education among the States, DHS, through U.S.-CERT, and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have launched a joint partnership to develop a series of national Web casts that will examine critical and timely cybersecurity issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.

U.S.-CERT also provides a method for citizens, businesses, and other institutions to communicate and coordinate directly with the U.S. Government on matters of cybersecurity. The private sector can use the protections afforded by the Protected Critical Infrastructure Information Act to electronically submit proprietary data to U.S.-CERT.

A.4.2 International Coordination on Cybersecurity

Cyberspace is ubiquitous and borderless. International cooperation in cybersecurity is an important way to foster national and joint international activities that promote a global culture of security and improve the

overall preparedness and incident response posture. The United States proactively uses its intelligence capabilities to protect the country from cyber attack, its diplomatic outreach and operational capabilities to build partnerships in the global community, and its law enforcement capabilities to combat cyber crime wherever it originates. These efforts require interaction with both policy and operational functions to coordinate national and international activity that is mutually supportive across the globe:

- **Global Culture of Cybersecurity:** DHS, in cooperation with the Department of State and other Federal agencies, engages in bilateral discussions with countries of interest, multilateral organizations and regional groups to raise awareness of cybersecurity issues and create a global culture of cybersecurity. DHS participates in bilateral discussions and programs with countries of interest and with nascent or emerging cybersecurity initiatives including Japan, Germany, Hungary, India, Italy, Korea, and others. DHS also provides leadership in regional groups, such as the Organization of American States (OAS) and the Asia Pacific Economic Cooperation (APEC), to raise awareness and develop cooperative programs on cybersecurity. For example, the OAS Committee on Counterterrorism has approved a framework proposal by its Cybersecurity Working Group to create an OAS regional computer incident response network that includes information sharing and capacity building. Multilateral collaboration to build global culture of security includes participation in the Organization for Economic Cooperation and Development (OECD), Group of 8, and United Nations. Many of these countries and organizations have developed mechanisms for engaging the private sector in their dialogue and program efforts, and the United States private sector has been actively involved.

- **International Collaboration in North America:** The United States engages with Canada and Mexico, as border neighbors, on critical infrastructure protection to enhance collaboration efforts on cybersecurity. Current activities include the United States, Canada and Mexico trilateral Security and Prosperity Partnership; the U.S.-Canada Critical Infrastructure Protection Framework for Cooperation (Smart Border Action Plan) and the U.S.-Mexico Critical Infrastructure Protection Framework for Cooperation (Border Partnership Action Plan). In both the multilateral and bilateral efforts, DHS and counterpart agencies in Canada and Mexico, respectively, have launched new Cybersecurity Working Groups to address critical information infrastructure issues of mutual concern.

- **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber crime, as well as: (1) the G8 High-Tech Crime Working Groups' principles for fighting cyber crime and protecting critical information infrastructure, (2) the OECD guidelines on information and network security, and (3) the United Nations General Assembly resolutions based on the G8 and OECD work. The goal of this outreach strategy is to encourage individual nations and regional groupings of nations to join DHS in efforts to protect the internationally interconnected national systems.

- **International Collaborative Arrangements:** The United States is working strategically with key allies on cybersecurity policy and operational cooperation. Leveraging the pre-existing relationships among computer security incident response teams (CSIRT), DHS has established a preliminary framework for cooperation on cybersecurity policy, watch and warning, and incident response on Critical Information Infrastructure Protection with key allies such as Australia, Canada, New Zealand, and the United Kingdom. The framework also incorporates efforts on key strategic issues as agreed upon by these allies.

  DHS is coordinating and participating in the establishment of an International Watch and Warning Network (IWWN) among cybersecurity policy, computer emergency response, and law enforcement participants of 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build global cyber situational awareness and coordinate incident response.

A.4.3 Training and Education

The National Strategy to Secure Cyberspace highlights the importance of cyberspace security training and education. Education and training are strategic initiatives in which DHS and other Federal agencies are actively engaged to affect a greater awareness and participation in efforts to promote cybersecurity for the future.

The Federal Government has undertaken several initiatives in partnership with research and academic communities to better educate and train future cybersecurity practitioners:

- DHS cosponsors the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program with the National Security Agency (NSA). Together DHS and NSA are working to expand the program nationally.
- DHS collaborates with the National Science Foundation (NSF) to co-sponsor and expand the Scholarship for Service (SFS) program, also known as the Cyber Corps program. The SFS program provides grant money to selected Centers of Academic Excellence in Information Assurance Education and other universities with programs of a similar caliber to fund the final 2 years of student bachelors, masters, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.
- In FY2004, the joint DHS/Treasury Computer Investigative Specialist (CIS) program trained 48 Federal criminal investigators in basic computer forensics. The agents from ICE, IRS, and USSS attended the basic six-and-a-half week course. This training was funded through the Treasury Executive Office of Asset Forfeiture (TEOAF). In FY2005, schools are scheduled for 72 more Federal investigators and 80 State and local officers.
- DHS is collaborating with the Department of Defense to finalize a comprehensive IT job skills standard to guide development of a national certification program for security professionals within the Federal Government and private industry.

A.4.4 Research and Development

The Cybersecurity Research and Development Act (2002) authorized a multiyear effort to create more secure cyber technologies, to expand cybersecurity R&D and to improve the cybersecurity workforce.

To further address cyber R&D needs, the White House Office of Science and Technology Policy (OSTP) established a Cybersecurity and Information Assurance Interagency Working Group (CSIA IWG) under the National Science and Technology Council (NSTC). The CSIA IWG was jointly chartered by the NSTC's Subcommittee on Networking and Information Technology Research and Development (NITRD) and the Subcommittee on Infrastructure. The Director of Cybersecurity R&D in the DHS S&T Directorate co-chairs this interagency working group, which includes participation from 20 organizations in 11 departments and agencies, as well as from several offices in the White House.

The purpose of the working group is to coordinate policy, programs, and budgets for cybersecurity and information assurance R&D. The CSIA IWG currently is engaged in developing the Federal Plan for Cybersecurity R&D, which includes near-term, mid-term, and long-term cybersecurity research efforts, in response to the *National Strategy to Secure Cyberspace* and HSPD-7. Specific examples include efforts to improve the security of fundamental protocols (such as Internet Protocol version six) and authentication technologies and to periodically review emerging technologies. DHS actively participates in CSIA IWG activities and continues to identify critical cyber R&D requirements for incorporation into Federal R&D planning efforts.

DHS and OSTP also facilitate communication between the public and private research and security communities to ensure that emerging technologies are periodically reviewed by the appropriate body

within the NSTC in the context of possible homeland and cyberspace security implications, and relevance to Federal research agenda.

A.4.5 New Partnership Programs and Exploring Private Sector Incentives

Awareness and understanding of the need for cybersecurity presents a challenge for Government and industry. Cybersecurity traditionally has been viewed as less tangible than physical security. When incidents occur that affect the CI/KR, physical impacts and response activities are clearly visible (e.g., smoke, power outages, more police presence on the street, barriers around buildings, etc.); however, in the cyber realm the impact and response activities are typically less obvious (e.g., slow Web page loading, compromised data, increased use of detection tools). Since cyber impacts and response activities are not readily seen or felt by large numbers of citizens, it is sometimes difficult to recognize the business case for cybersecurity. Often the cost of cybersecurity is perceived as being too high, with the resulting consequences of a successful cyber attack not fully understood by individuals. Although cybersecurity does require significant investments in time and resources, the cost of an effective cybersecurity program is likely to be lower than that of a successful cyber attack. Increased awareness is needed to educate public and private infrastructure owners and operators of the risks associated with cyber attacks and to provide the motivation for sufficient investment in cybersecurity programs.

To date, DHS has engaged with infrastructure owners and operators on a number of cybersecurity initiatives. Through programs such as U.S.-CERT, CSSC, outreach to ISACs and industry associations, and the Software Assurance Program, DHS is working with the public and private sector to foster collaboration and promote awareness of cybersecurity risks and create incentives for increased investment in cybersecurity.

Appendix B: Summary of Relevant Authorities

This summary outlines information contained in *Federal NIPP Authorities: Linkages to Statutes, Policy, and Other National Plans*, created for the NIPP Council Policy and Planning Working Group (February 2005), which provides an overview of relevant Federal authorities, including the Federal legislation, policy, and plans that are directly or indirectly related to the NIPP and identifies relationships between each of these authorities.

B.1 Statutes

Clean Water Act (October 1977)

Comprehensive Environmental Response, Compensation, and Liability Act (December 1980)

Defense Production Reauthorization Act of 2003 (December 2003)

Federal Information Security Management Act (December 2002)

Gramm-Leach Bliley Act (1999)

Homeland Security Act of 2002 (November 2002)

Intelligence Reform and Terrorism Prevention Act of 2004 (December 2004)

Maritime Transportation Security Act of 2002 (46 USC § 70101, et seq.)

Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (June 2002)

Sarbanes-Oxley Act (2002)

Stafford Disaster Relief and Emergency Assistance Act (October 2002)

B.2 Homeland Security Presidential Directives

HSPD-1: Organization and Operation of the Homeland Security Council (October 2001)

HSPD-2: Combating Terrorism through Immigration Policies (October 2001)

HSPD-3: Homeland Security Advisory System (March 2002)

HSPD-4: National Strategy to Combat Weapons of Mass Destruction (WMD) (December 2002)

HSPD-5: Management of Domestic Incidents (February 2003)

HSPD-6: Integration and Use of Screening Information (September 2003)

HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003)

HSPD-8: National Preparedness (December 2003)

HSPD-9: Defense of United States Agriculture and Food (February 2004)

HSPD-10: Biodefense for the 21st Century (April 2004)

HSPD-11: Comprehensive Terrorist-Related Screening Procedures (August 2004)

HSPD-12: Policy for a Common Identification for Federal Employees and Contractors (August 2004)

HSPD-13: Maritime Security Policy (December 2004)

HSPD-14: Domestic Nuclear Detection (April 2005)

B.3 Other Federal Plans

National Response Plan (including the Federal Response Plan and the Federal Radiological Emergency Response Plan) (December 2004)

National Oil and Hazardous Substances Pollution Contingency Plan (1968)

National Plan for Research and Development in Support of Critical Infrastructure Protection (December 2004)

Interagency Security Plan (June 2004)

Appendix C: Standards for Risk, Consequence, and Vulnerability Assessments

This appendix provides the standards and the minimum characteristics that a consequence, vulnerability, or risk assessment methodology should observe in order to be used in place of the standard risk analysis methodology, *Risk Analysis and Management for Critical Asset Protection* (RAMCAP).

As detailed in Chapter 3, DHS is using a risk management framework to facilitate the allocation of the national resources available for CI/KR protection. The backbone of this framework is the assessment of the consequences, vulnerabilities, and risks associated with nationally critical infrastructure, and the identification and implementation of protective measures to reduce those factors.

Currently, DHS, in conjunction with representatives from private industry, is developing an overarching guidance document and sector-specific implementation documents (or "modules") under the rubric of the RAMCAP. It is the consequence and vulnerability assessment methodology recommended by DHS for use in CI/KR protection efforts. The results obtained through the implementation of the RAMCAP consequence and vulnerability assessments are then used to feed the Federal Government's comparison of risk across sectors. Of primary importance in the RAMCAP methodology is the use of common terminology, common working assumptions, and common metrics to allow assets from different CI/KR sectors to be compared with one another based on risk. It is these commonalities that will allow the prioritization of CI/KR assets necessary for the optimal allocation of finite CI/KR protection resources.

Ideally, all asset owners and operators will use the RAMCAP methodology to assess their assets once the methodology is finalized. This would facilitate the cross-sector comparison of assets based on risk and the compilation of a true national risk profile. However, the Federal Government is well aware of the fact that dozens, if not hundreds, of alternative consequence, vulnerability, and risk assessment methodologies currently exist and are being employed by asset owners and operators across all 17 CI/KR sectors. In order to minimize the burden on asset owners and operators, where possible, DHS will work to use the results from these other assessments to support a national comparative risk analysis and the associated cross-sector prioritization of assets. This would preclude the need for additional assessments using the RAMCAP methodology from owners and operators who already have performed comprehensive consequence and vulnerability analyses on their assets. Yet, in order to do so, the assessment methodologies used by asset owners and operators must meet the standards specified in this section and pass a quality check to ensure a minimal level of robustness and contain certain characteristics in common with RAMCAP so that their results are comparable to the results developed by RAMCAP and other accepted methodologies.

The remainder of this appendix will provide some broad guidelines that describe the general approach a consequence, vulnerability, or risk assessment methodology should follow to conform to anticipated DHS standards, as well as some minimal characteristics that an acceptable methodology should contain. As the RAMCAP methodology is refined, DHS will update this appendix to reflect in greater detail the specific standards that a methodology must contain to produce results that can be used for the cross-sector prioritization of assets envisioned as part of the national comparative risk analysis.[17]

C.1 Overarching Risk Assessment Standards for CI/KR Protection Activities

Risk can be defined in a variety of ways depending on the circumstances. For example, risk has a very different meaning in the financial world than it does in the world of safety. In the realm of critical

[17] The standards being developed are being derived from well-accepted risk analysis principles; thus most legitimate, robust assessment methodologies currently being employed by CI/KR owners and operators are likely to meet the forthcoming requirements as is, or will be able to do so with minimal refinement.

infrastructure protection, risk is defined as a function of three factors: consequences, vulnerability, and threat.

For the purposes of the national comparative risk assessment, determination of threat is the purview of the Federal Government. However, determining the remaining two factors, consequences and vulnerability, can be most efficiently and accurately accomplished by asset owners and operators. Accordingly, for a risk assessment methodology to meet the standards required for input into the Federal Government's overarching risk assessment framework, it must include assessments of both consequences and vulnerabilities.

In addition to having to examine both consequences and vulnerabilities, an acceptable risk assessment methodology must meet certain minimal standards to ensure the quality and robustness of the methodology. These same standards apply equally to consequence and vulnerability assessments as well. While DHS will provide a more specific listing of these standards, the following list of attributes, drawn from the Center for Chemical Process Safety's SVA quality check, provides a list of attributes an acceptable methodology would possess:

- **Completeness:** Provides reasonably complete results via a systematic and rigorous process
- **Integrity:** Is based on classical risk analysis and security vulnerability analysis theory
- **Reproducibility:** Provides results that are reproducible by equivalently experienced personnel
- **Transparency:** Easily understandable to others as to how it was accomplished, the assumptions used, and the basis for risk decisions
- **Documented:** Provides clear and complete documentation of the methodology and the products from its use
- **Defensible:** Thorough and professional; addresses relevant concerns of Government regulations, employees, and the public
- **Precision:** The results are free from obvious errors or omissions so that results are suitable for decisionmaking

Risk assessment methodologies that possess these traits and assess both consequences and vulnerabilities should produce results that can be used by the Federal Government in determining how to allocate its limited CI/KR protection resources.

C.2 Minimal Standards for Consequence Assessments

For a consequence assessment to produce results that can be used as part of the determination of the national risk profile, it must be comparable to RAMCAP and other acceptable methodologies in three primary areas: (1) the types of consequences assessed, (2) the methods of measurement of the various consequences, and (3) the assumptions used in calculating the potential consequences. The remainder of this subsection contains some general guidance that can be used in the interim while the RAMCAP methodology is refined.

C.2.1 Types of Consequences Assessed

The first step in ensuring consistency among consequence assessment methodologies is to ensure that the types of consequences assessed are comparable. For DHS, the consequences of interest are the consequences of national significance set forth in Homeland Security Presidential Directive 7.[18] Those consequences typically are divided into four main categories:

[18] Paragraph (7), sections (a) through (f) of HSPD-7.

- **Health Impact:** Effect on human life and physical well-being (e.g., fatalities, injuries);
- **Economic Impact:** Effect on the local, State, Territorial, tribal, regional, or national economy (e.g., cost to rebuild asset, cost to respond to and recover from attack);[19]
- **Psychological Impact:** Effect on the public's morale and confidence in national economic and political institutions; and
- **Governance Impact:** Effect on the national Government's ability to maintain order, deliver minimum essential public services, ensure the public's health and safety, and carry out national security-related missions.

While an ideal consequence assessment methodology would take into consideration all four primary categories of consequences, accurately estimating potential psychological or Government impact can be very difficult, and is often beyond the abilities of an individual asset owner/operator. Accordingly, for a consequence assessment methodology to be acceptable, it simply must, at a minimum, address both the health and direct economic consequences of an attack.

C.2.2 Methods of Measuring Consequences

Consequences typically can be measured either quantitatively or qualitatively. Health and economic impacts generally lend themselves to quantitative measurement (e.g., number of lives lost cost in dollars of rebuilding an asset), whereas psychological and governance impacts are more often measured qualitatively.

When quantitative measures are used, the results typically are placed into bins to allow for more general comparison. For instance, $0 to $10,000 in damages may result in a score of 1 for economic impact, $10,001 to $100,000 in damages may result in a score of 2 for economic impact, and $100,001 to $1,000,000 may result in a score of 3 for economic impact, and so on.[20] However, there are many different ways in which these bins (collectively referred to as "scales") can be set up. The same issue occurs when numbers are used to represent a quantitatively measured impact (e.g., no impact to national psyche is a score of zero, minimal impact to national psyche is a score of 1, moderate impact to national psyche is a score of 2, and so on). In order to ensure comparability of consequence assessment results using various methodologies, the methodologies must employ consistent scales. DHS is developing a standardized rating table (or national scale) to be used to ensure consistent assessments of consequence across sectors.

C.2.3 Assumptions Used in Estimating Potential Consequences

When estimating potential consequences, numerous assumptions must be made. Examples of assumptions made during consequence analysis include the estimated level of success of a given scenario (e.g., worst-case vs. worst reasonable case v. most likely) and the type of attack considered (e.g., successful detonation of a nuclear bomb at the asset v. successful detonation of a car bomb at the asset). For consequence assessment results to be comparable, the methodologies must employ similar assumptions.

[19] When the Federal Government considers economic impact, it takes into account both direct and indirect economic impact, including cascading effects on the local, State, regional, and National economies. While an ideal consequence assessment takes indirect/cascading effects into account, the Federal Government realizes that the ability to accurately estimate these impacts often is beyond the capability of an individual asset owner/operator, and thus this is not a prerequisite for an assessment methodology to be considered robust.

[20] Note, the bins/scaling used in this example are purely hypothetical and to be used for explanatory purposes only; they do not represent an actual scale being used by the Federal Government at this time.

C.3 Minimal Standards for Vulnerability Assessments

Vulnerability assessments evaluate the extent to which identified assets are susceptible to various types of threats and attack scenarios. The suite of tools that DHS is developing and using for vulnerability assessments is scenario-based, which means that the assessments measure the susceptibility of an identified asset to a specific threat scenario. This allows the assessment to be informed in general terms by adversary tactics and weapons. Consequently, for the results of any vulnerability assessment methodology to be acceptable for DHS cross-sector analysis purposes, the assessment methodology should be scenario based and certain minimum scenarios or their equivalent must be used. Once the RAMCAP SVA methodology is refined, the list of required scenarios can be provided.

Additionally, in evaluating the extent to which an asset is vulnerable, and thus likely to suffer particular consequences as the result of the successful execution of a terrorist attack, an acceptable security vulnerability assessment must consider the existing measures that are in place to reduce that asset's exposure to the scenario threats. Specifically, security specialists should examine the ability of an asset's existing security profile to deter, detect, devalue, defend against, mitigate, respond to, and recover from the threat scenarios. Accordingly, acceptable vulnerability assessments will consider the following asset capabilities:

- **Deterrence Capabilities:** The ability to deter an attack by affecting the adversary's perception of its capability or the level of effort required to execute a successful attack.
- **Detection Capabilities:** The ability to identify or expose an attack before it takes place.
- **Devaluing Capabilities:** The ability to reduce the attacker's incentive to attack by reducing the value of the target.
- **Defensive (Delay and Denial) Capabilities:** The ability to prevent an attack or delay it long enough for security or law enforcement personnel to mount an effective response.
- **Response Capabilities:** The ability to effectively respond to an attack under way.
- **Consequence Reduction/Mitigation Capabilities:** The ability to limit consequences should an attack occur.
- **Recovery Capabilities:** The ability to return to an acceptable level of operations after an attempted or successful attack.

When evaluating asset capabilities, many security vulnerability assessments focus solely on physical security; however, physical security is only one aspect of a complete, robust vulnerability assessment. To be acceptable to DHS for national comparative risk assessment purposes, a vulnerability assessment must look not only at an asset's physical security, but also must consider personnel security and other human security issues, cybersecurity and network architecture issues, operational security, and infrastructure dependencies and interdependencies.

Finally, in order to compare the results of vulnerability assessments across asset types, a scoring system must be utilized much like the bin or scaling systems used to measure consequences. Thus, in order to support the comparison of vulnerability assessment results, DHS is developing a standardized rating table as part of the RAMCAP process that can be used to ensure consistent assessments of vulnerability across sectors.

Appendix D: Established Coordination Mechanisms

Coordination	Mechanism	Description
Local to Local	Inter-Local Agreements	Cities and towns can exchange information and cooperate on any number of projects. Inter-local agreements are a mechanism to do cooperatively anything that can be done as an individual municipality.
	Mutual Aid Agreements	Establishes means through which one local government can offer and another receive assistance in a time of disaster. These agreements cover logistics, deployment, liability, reimbursement and many other issues. The idea, of course, is to provide assistance in the most efficient manner possible by having the conditions worked out in advance.
	County Commissioners	Because counties are the level of government closest to the people and serve all the people of the State, county commissioners provide leadership, services and programs to meet the health, safety and welfare needs of their citizens.
Regional	Councils of State Governments	Regional councils, by law, are political subdivisions of the State with the authority to plan and initiate needed cooperative projects but they do not have powers to regulate or tax, which are exclusively assigned to cities and counties. A council's duties include comprehensive planning for regional employment and training needs, criminal justice, economic development, homeland security, emergency preparedness, bioterrorism, 911 service, solid waste, aging, transportation and rural development.
Local to State	Committees, Commissions, and Boards	Local to State legislative- and regulatory-level interaction occurs through State committees, commissions, and boards dealing with environmental, transportation, community development, retirement, insurance, and many other issues. This also includes working with the office of the Governor and Homeland Security Advisor.
Local to Federal	National League of Cities	Ensuring that residents can live and work in a safe and healthy environment is one of the highest priorities that cities have. The National League of Cities works with local elected officials to ensure that there is full Federal funding for both traditional public safety programs and homeland security activities.
State to State	Interstate Compacts	States face issues that are not confined to geographical boundaries or jurisdictional lines. Interstate compacts are a mechanism that can be used to address sector interdependencies and coordinate protection of CI/KR. Compacts are organized in a number of ways: • Sector-Based: Western Interstate Energy Compact • Preparedness: Interstate Mutual Aid Compact • Regional: Canadian River Compact For more information on interstate compacts, contact the National Center for Interstate Compacts (NCIC): http://www.csg.org/CSG/Programs/National+Center+for+Interstate+Compacts/default.htm
Federal to Federal	Memoranda of Understanding or Agreement	Agreements between Federal departments and agencies to cooperate on a specific topic or initiative.

Appendix E: Sector-Specific Plan Structure and Content

The SSPs follow a consistent structure to facilitate cross-sector comparisons and to enable coordination among security partners. Each plan includes the following structure:

Chapter 1: Sector Background & Engagement - In this chapter of the SSP, SSAs characterize their sector, describe the context in which the SSA engages with the security partners, and identify authorities and regulations relevant to protective activities. It also provides a sector "snapshot" that highlights sector-specific threats, as well as structural, regulatory, and other sector characteristics needed to be considered in risk management decisions. DHS uses this information to understand how the SSA views its sector responsibilities, to obtain information on the key security partners in the sector and how they relate to each other, and to determine legal authorities for implementing the program. Information in this chapter is organized into the following sections:

1A. **Sector Profile:** Includes a concise definition of sector boundaries and characteristics of assets, discussion of any overlaps in scope between sectors and how they are addressed, characterization of the sector assets including, where appropriate, sub-categorizations or classes of assets, particularly if the sector includes obviously distinct types of operations, businesses, facilities, etc., and a description of the entities that own or operate the various assets or classes of assets.

1B. **Review of Authorities:** Information on governing authorities (e.g., laws, rules, regulations, etc.) applicable to the protection of assets within the sector, and any gaps in authorities that could hinder the CI/KR protection process, pertinent to: collection of information, information sharing and protection, vulnerability assessment, and protective strategies.

1C. **Mapping Relationships:** Status of current sector security partner relationships that identify successful efforts, recognize the complexity and diversity of sectors that require active subcomponents, and target areas where further outreach is desired and assistance from DHS may be helpful; description of sector relationships, as well as the roles and responsibilities of security partners which include private sector owners/operators and organizations, other Federal departments and agencies, State and local agencies, and international organizations and foreign countries.

1D. **Coordinating Structures:** Structures through which the sector will be coordinated by the SSA including: all NIPP-related coordinating mechanisms and structures, whether public or private; relationships of coordinating mechanisms and structures; and basic concept of operations. At a minimum, these structures include:

- ***NIPP Coordination Councils*:** Composition of sector GCCs, SCCs, frequency of meetings, and progress in establishing these councils as sector management for the sector-specific risk-reduction planning and activities
- ***State, Territorial, Local, Tribal Governments:*** Role in sector operations; safety and security, and risk reduction planning and activities; and level of integration of these entities in the sector

1E. **Information Sharing Mechanisms:** Structures and mechanisms through which information will be shared within the sector and with other sectors and DHS; include examples of information-sharing and communication mechanisms developed by DHS to ensure that protection programs are operationally coordinated, and that threat and other security-related information is shared with appropriate security partners.

Chapter 2: Establish Sector-Security Goals: This chapter of the SSP provides the vision and goals for the sector's protective efforts. Each sector has distinct assets, operational processes, business environments, and risk management approaches that determine the security vision and goals that the sector will pursue. Such goals reflect the overall risk management outcomes that owners/operators and government leaders seek to produce for their sectors. Information in this chapter is organized into the following sections:

2A. **Process to Establish Sector-Security Goals:** Summary of the process used to develop the vision and goals in the SSP and how they will be re-evaluated as the sector changes.

2B. **Sector-Security Goals and Objectives:** The outcome of the process in terms of the agreed upon sector security vision, goals, and any associated objectives.

Chapter 3: Identify Sector Assets: In this chapter the SSP, the process used to gather and maintain information on sector assets is described. In this context, asset identification focuses on those assets or systems that are large enough to be considered targets for attack and that may potentially be candidates for protective actions. They also must consider assets located in foreign countries, cyber (as well physical) characteristics, dependence and interdependence of assets, and grouping of assets as systems. Information in this section is organized into the following sections:

3A. **Process to Identify Sector Assets:** Current or proposed approaches to identify sector assets, data sources of such information, and plans to validate such inputs, as follows:

- *Defining Asset Data Parameters*: Defining the specific information that will be collected about each asset (taking a comprehensive, integrated view of the asset to include the characteristics, dependencies, and interdependencies, international links, and cyber systems needed for it to function), how the sector defines the universe of assets (including subsectors), and the threshold level to be used in identifying assets of consequence requiring further analysis, and why this level is appropriate.
- *Collecting Asset Data*: Process for collecting or obtaining access to this information, currently and in the future (as the information will constantly change) to include: identifying currently available information on sector and cross-sector assets; formatting, linking, and delivery of data to DHS; gathering the information required to inventory a sector's infrastructure beyond the SSA's current holdings; location of asset data storage; information protection mechanisms; and frequency of update to asset information.
- *Verifying Asset Data*: Quality control process for ensuring that information collected is reliable to include process to verify asset information; protocol for reviewing data (e.g., sample size, criteria, frequency), steps to address incomplete and/or inaccurate data, and follow-up activities required based on the infrastructure's significance (e.g., onsite meetings, validation of owner/operator procedures, etc.).

3B. **Updating Asset Data:** Process for ensuring access to continuously updated asset data for the sector: frequency of updates (e.g., as changes occur and/or on a routine basis); delivery of updated information; considerations for reevaluation of the sector inventory itself; sector partner responsible for obtaining the data; notice of data updates; and maintenance of asset information (e.g., by who and at what frequency).

3C. **Protecting Asset Data:** Process of protecting asset data to include: security classification and a description of asset information protection mechanisms that are in place or planned.

Chapter 4: Assess Sector Risks: Current approach for assessing risks to sector assets, how assessment methods unique to the sector can be reviewed and, if necessary, modified to allow compatibility with assessment methods and data from other sectors, as well as how this information will be provided to

and/or shared with DHS; discussion of each sector's strategy to help coordinate and implement a common risk management vocabulary, common threat scenarios, common scales, and generally-accepted risk assessment practices; and process for:

- Selection of assets for further analysis;
- Identifying and collecting current vulnerability and risk assessment data;
- Identifying and assessing sector-specific tools;
- Building a risk analysis capability;
- Encouraging security partner implementation; and
- Assisting in dependency and interdependency analysis.

Chapter 5: Prioritize: Discussion of a validated assessment of component risk factors (threat, vulnerabilities, and consequence) with their known inter- and intra-sector dependencies and interdependencies to produce an ordered assessment of those assets representing national risk.

Chapter 6: Implement Protective Programs: Discussion of current or proposed processes for developing protective programs to implement their selected strategies; describe:

- **Sector Security Strategies:** Balance of prevention, protection, response, and recovery by sector, sub-sector, or asset class and how they influence guidelines or minimum standards for protective actions.
- **Decisionmaking Processes:** For assessing anticipated costs of protective actions, including purchasing data sources, for balancing costs against the risks for particular assets, and the role of security partners in carrying out these analyses.
- **Protective Program Implementation:** Description of protective actions that are appropriate for the sector and why (tie into goals); how sector-specific protective actions are coordinated with actions implemented by DHS; who conducts protective programs and under what circumstances; how protective actions are tracked; and use of best practices and information sharing in encouraging security partner implementation; roles and responsibilities of sector security partners; how critical information generated from plan implementation, particularly the information on which assets appear to pose the highest risk, will be considered; how security partners will share best practices for long-term protective programs, including overcoming implementation challenges; and how often and by which entity the protective programs will be updated and refined.

Chapter 7: Measure Progress: Description of performance metrics for the implementation of the SSP based on NIPP metrics; process for reporting on metrics and overall progress of sector initiatives to DHS.

7A. **Process to Develop Sector-Specific Metrics:** Development of sector-specific metrics based on its CI/KR protection goals to result in a short, focused, and manageable list of process and outcome metrics, organized by asset class if appropriate.

7B. **Reporting Responsibilities:** Description of responsibilities and timeframes for meeting HSPD-7 annual reporting requirement to the Secretary of Homeland Security as well as any other reporting required as part of the NIPP.

7C. **Continuous Improvement:** Description of how the sector will continuously refine CI/KR protection efforts to improve the security of sector CI/KR including processes to:

- Use metrics to compare performance to goals;
- Revise approaches in the SSP to reflect activities and progress;

- Identify and improve upon protection of assets that warrant additional resources or other changes;
- Focus CI/KR protection efforts on addressing areas of concern; and
- Collect and share how lessons learned and best practices with security partners and DHS.

Chapter 8: Plan CI/KR Protection Research and Development: Explanation as to how the sector will strengthen the linkage between sector-specific and national R&D planning efforts, technology requirements, current R&D initiatives, gaps, and candidate R&D initiatives.

8A. **Sector Technology Requirements:** Process to identify sector technology requirements and communicate them to S&T/OSTP for inclusion in the Federal CIP R&D Plan on an annual basis; and a summary of technology requirements.

8B. **Current R&D Initiatives:** Process to annually solicit a listing of current Federal R&D initiatives from S&T/OSTP that have potential to meet sector CI/KR protection challenges; and a description of how this listing will be analyzed to indicate which initiatives have the greatest potential for positive impact.

8C. **Gaps:** Process for conducting an analysis of the gaps between the sector's technology needs and current R&D initiatives from S&T/OSTP.

8D. **Candidate R&D Initiatives:** Process to determine which candidate R&D initiatives are most relevant for the sector and how these will be summarized.

Appendix F: Sector Security Vision Statements

Each sector has defined a security vision that articulates desired end state for their infrastructure protection posture. The vision forms the basis for the sector security goals as included in each SSP. The security vision for each of the 17 CI/KR sectors is presented in the sections that follow.

F.1 Agriculture and Food Sector

The Agriculture and Food Sector accounts for roughly one-fifth of the Nation's economic activity and has the capacity to provide food and clothing to people beyond the U.S. borders. Almost the entire sector is privately owned. The sector is overseen at the Federal level by the U.S. Department of Agriculture (USDA) and the U.S. Department of Health and Human Services' Food and Drug Administration (FDA). The sector covers agricultural production from pre-harvest through postproduction and national forest lands, the animal feed industry, and food facilities. The sector includes an estimated 2.1 million farms, with an average of 441 acres. In addition, the sector includes an estimated 880,587 firms and 1,086,793 facilities.

The Agriculture and Food Sector is dependent on the Drinking Water and Wastewater Treatment Systems Sector for clean irrigation and process water, the Transportation Systems Sector for movement of products, and the Energy Sector to power the equipment needed for agriculture production and food processing.

Sector Security Vision:

The Food and Agriculture Sector will work to create and continue a government-private sector partnership to prevent the contamination of the food supply that would pose a threat to public health, safety, and welfare. The Food and Agriculture Sector will provide the central focus for a steadily evolving and complex industry/sector, with particular emphasis on the protection and strengthening of the Nation's capacity to supply safe, nutritious, and affordable food. In doing so, the Sector will ensure that the industry has incorporated the concepts of HSPD-5, 7, 8, and 9 in their own critical asset protection plans, vulnerability/risk reduction plans, and continuity of operations plans. The Sector will provide leadership on food, agriculture, natural resources, and related issues based on sound public policy, the best available science, and efficient management.

F.2 Banking and Finance Sector

The Banking and Finance Sector, the backbone of the world economy, is a large and diverse sector primarily owned and operated by private entities. The banking system consists primarily of Federal and State-chartered depository institutions. In most cases, Federal regulators have at least some authority over these institutions. Key banking system assets include retail facilities, ATM networks, Automated Clearing House operators, Federal Reserve Banks, and the Electronic Payments Network. Credit and liquidity markets are not formal markets with either a physical location or one narrow set of methods that define them, yet they are fundamental to the operation of the U.S. economy and to Federal and State Governments. Investment products are offered by a wide variety of financial institutions such as securities firms, depository institutions, pension funds, and government- sponsored enterprises. Risk transfer products are offered by insurance companies, futures firms, and forwards participants.

Financial services firms provide a broad array of financial products that (1) allow customers to deposit funds and make payments, (2) provide credit and liquidity, (3) allow customers to invest funds for both long and short periods, and (4) transfer financial risks between customers.

While the sector is overseen at the Federal level by the U.S. Department of the Treasury, two organizations advise on infrastructure protection to the financial services industry:

- The Financial and Banking Information Infrastructure Committee (FBIIC), chaired by the Department of the Treasury and composed of Federal and State financial regulatory agencies, coordinates efforts to prepare for and respond to cyber or physical attacks against the Financial Sector.
- The Financial Services Sector Coordinating Council (FSSCC), composed of private-sector trade associations, fosters and coordinates sector-wide voluntary initiatives to improve critical infrastructure protection.

The Department of the Treasury and the FBIIC have identified a number of systemically critical institutions whose operations form the backbone of the financial system.

The Banking and Finance Sector is dependent on the Telecommunications, Energy, Information Technology, and Transportation sectors. Telecommunications and information technology are integral to the efficient operation of financial institutions. The power outage of August 2003 demonstrated energy's importance to the sector, and the transportation sector enables customer and employee access to financial facilities and is critical to sending and receiving goods and services in the everyday conduct of business. There are also interdependencies with international service providers and foreign markets.

Sector Security Vision:

The Department of the Treasury, as SSA for the Banking and Finance Sector, will continue to lead national efforts to ensure that the protection of sector infrastructure is effectively coordinated. The Treasury Department will continue its partnership with Federal, State, and other financial regulators, and the private sector, that are essential to ensuring a resilient national economy. The Treasury Department will continue to lead efforts to ensure effective information sharing to, from, and within the Banking and Finance Sector, using mechanisms such as the Financial Services Information Sharing and Analysis Center.

F.3 Chemical Sector

The Chemical Sector is an integral component of the U.S. economy, employing nearly one million people, and earning revenues of more than $460 billion a year. Participants in the Chemical Sector view themselves as falling into one of four main segments, based on the end product produced: (1) basic chemicals, (2) specialty chemicals, (3) life sciences, and (4) consumer products. There are several hundred thousand "chemical facilities" in the U.S., encompassing everything from production facilities to hardware stores. The great majority of these facilities are privately owned, requiring DHS, as the SSA, to work closely with the private chemical industry and its industry associations in order to identify assets, assess vulnerabilities, prioritize assets, develop protective programs, and measure program effectiveness.

From a homeland security perspective, the most pressing concern in the Chemical Sector is the potential for terrorists to attack assets in such a way as to create harmful consequences to public health and safety. More than 15,000 U.S. facilities produce, use, or store more than 140 chemicals that, when present above certain threshold amounts, have the potential to pose great risk to human health and the environment if released. Thus, ensuring risk reduction for toxic inhalation hazards has been a leading DHS priority in this sector. The potential economic impact of a successful terrorist attack against the Chemical Sector is also a major concern. Only one Federal law, the Maritime Transportation Security Act of 2002 (46 USC § 70101, et seq.), establishes direct authority concerning terrorism-related security at chemical facilities in the maritime domain. Consequently, the decision to secure chemical facilities overwhelmingly lies with the individual asset owners and operators, although a few States and localities have begun enacting regulations addressing chemical facility security. In addition, a considerable number of Federal laws impose safety or other requirements on the production, storage, use, and transportation of chemicals; these laws indirectly help secure chemical facilities.

Sector Security Vision:

The Chemical Sector is dedicated to building an economically-competitive industry that has achieved a sustainable security posture via a uniform, high-order strategic approach to risk reduction, protective measure implementation, information sharing, and verification of compliance to standards.

F.4 Commercial Facilities Sector

Commercial facilities, sometimes known as "soft targets," are potential targets for terrorist attacks because they are especially vulnerable and may be subject to large casualties and economic damage. Due, in part, to accessibility, commercial facilities are very difficult to defend against terrorist attacks. The Commercial Facilities Sector comprises a number of asset categories, including hotels, commercial office buildings, public institutions (e.g., museums, libraries, zoos), convention centers/stadiums, theme parks, schools, hospitals, colleges, apartment buildings, restaurants, and markets. Any commercial facility or soft target accommodating large groups of individuals in a public or semipublic place qualifies for inclusion in the Commercial Facilities Sector.

With more than 53,000 hotels, 46,000 shopping centers, and 1,300 stadiums/arenas, DHS expects that industry associations will provide the primary conduit for security partner interaction. For example, the International Association of Assembly Managers is a valuable conduit to owners of sports stadiums and convention centers. Another important player is the Real Estate Information Sharing and Analysis Center (RE-ISAC), composed of major national real estate trade associations. The RE-ISAC facilitates information sharing on terrorist threats, vulnerability assessments, and response planning.

Sector Security Vision:

The commercial business and community facilities sub-sector are dedicated to enhance protective security for individual assets and prioritize those assets most at risk, in order to deter and defend against terrorist attacks aimed at their facilities.

The commercial industrial facilities sub-sector are dedicated to enhance protective security for individual assets to deter and defend against terrorist attacks to ensure the availability of raw materials and the distribution of finished products essential to the national economy.

F.5 Dams Sector

The term "dam" includes levees, conventional dams, navigation locks, canals (excluding channels), or other similar types of water retention structures. Man-made dams may be classified according to the type of construction material(s) used, the method(s) of construction, the slope or cross section of the dam, the way the dam resists the forces of the water pressure behind it, the means used for controlling seepage, and the purpose of the dam. Materials used for construction of dams include earth, rock, tailings from mining or milling, concrete, masonry, steel, timber, miscellaneous materials, such as plastic or rubber, and any combination of these materials. The two most typical types of dams in use today are embankment dams and concrete dams (gravity and arch dams).

The majority of dams in the U.S. (66%) are owned by private entities. However, very large dams, or dams with a reservoir storage of greater than one million acre-feet, are mostly owned by the Federal Government. Companies or cooperatives privately own most medium-sized dams, that is, dams with reservoir storage of 100 to 10,000 acre-feet. Medium-sized dams are used for irrigation, water supply, hydroelectric power, and direct hydropower. A small percentage of medium-sized structures are non-Federal hydropower dams licensed by the Federal Energy Regulatory Commission (FERC). Most small dams (those storing less than 100 acre-feet of water) are privately owned.

Key interdependencies with other sectors include the hydroelectric portion of the Energy SSP and the Drinking Water and Wastewater Treatment Systems SSP. It should be noted that some large dams, such

as Hoover Dam, also are symbolic national icons whose security presents specific challenges when juxtaposed with the need to balance open visitor access.

Sector Security Vision:

The Dam Sector will detail the protective measures and policies necessary to protect these assets from terrorist acts through the development of multifaceted and multi-level security programs specifically designed to accommodate the variety and mission of this sector. The Dam Sector, by fostering and guiding research in the development and implementation of protective measures, will ensure the continued economic use and enjoyment of the national infrastructure entrusted to its care in an economically sound manner through the use of a risk-based management program of mitigation, preparedness, response, and recovery.

F.6 Defense Industrial Base Sector

The Defense Production Act of 1950, Executive Order 12919, and DOD Directive 5000.60 are all focused primarily on ensuring adequate industrial capacity for national security. Presidential Decision Directive 63 identified national defense as a special function of interest in the context of Critical Infrastructure Protection in 1998. The July 2002 *National Strategy for Homeland Security*, the February 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, and the December 17, 2003, *Homeland Security Presidential Directive 7* (HSPD-7), all identify the Defense Industrial Base (DIB) as a critical infrastructure sector and assign the responsibility for ensuring DIB functionality to the Department of Defense.

The DIB sector security partners include the DOD, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, production, and maintenance of military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes more than 100,000 companies and their subcontractors who perform under contract to DOD and companies providing incidental materials and services to DOD, as well as Government- Owned, Contractor-Operated and Government-Owned, Government-Operated facilities. DIB companies include both domestic and foreign entities, some with operations located in many countries.

The DIB provides defense-related products and services that are essential to mobilize, deploy, and sustain military operations. The DIB does not include commercial infrastructure that provides, for example, power, communications, transportation, and other utilities that DOD war fighters and support organizations use to meet their respective operational needs. These activities, including cyber, are addressed in DOD's broader Defense Critical Infrastructure Program (DCIP) and are integrated in all DIB sector activities.

DIB owners and operators protect DIB assets from many potentially hostile threats and hazards. However, the DIB has limited authority, or in many cases no authority, to perform law enforcement functions or to take offensive protective action. Critical assets within the DIB are potentially vulnerable to exploitation that could result in DOD mission degradation or failure. The fact that the DIB exists in an open, global environment exacerbates the susceptibility of critical DIB assets to vulnerability exploitation.

The changing composition of the DIB (e.g., resulting from mergers and acquisitions) and the evolving regulations and policy that govern the relationship of DOD to the DIB necessitates broad-based, continuing, long-term interaction and collaboration with DIB members to ensure DIB capability and reliability. This long-term continuing interaction is vital as the vast majority of critical DIB assets reside in the private sector.

Sector Security Vision:

The Defense Industrial Base Sector will focus on facilitating the resiliency of critical private and public sector defense industry assets and systems whose disruption could hinder the execution of defense

mission essential functions. Further, the sector will pay particular attention to preventing and remediating cascading failures by ensuring that interdependent systems can survive any hazard.

F.7 Emergency Services Sector

The Emergency Services Sector (ESS) consists of five disciplines: fire and hazardous material, search and rescue, emergency medical services, law enforcement, and emergency management. All first responders within ESS are individuals possessing specialized training from one or more of these five disciplines. They are the men and women who serve in every community in the U.S., protecting citizens, ensuring order in communities, saving lives, and working to restore essential services to homes and communities in times of disaster, natural or otherwise.

The ESS is a system of response elements that forms America's first line of defense and prevention in any terrorist attack. The core elements of the ESS are not found in large, complex structures or facilities, but in the highly trained forces of professionals, organized and equipped to conduct high-risk operations in times of emergency. The ability of the Nation to protect all CI/KR is heavily dependent on these men and women who serve in the Nation's emergency services. Their protection is fundamental to preserving America's way of life.

Sector Security Vision:

The Emergency Services Sector strives to protect the people, police, fire, rescue, emergency medical technicians, emergency management services, physical components, and systems necessary to effectively save lives, protect all of the Nation's Critical Infrastructure/Key Resources, other property and the environment, assist communities affected by disasters, and aid in the recovery from emergency situations. To accomplish this, the Sector will undertake a detailed risk assessment program and use the results of their analyses to ensure that their mission critical resources are always available to the public.

F.8 Energy Sector

The U.S. energy infrastructure fuels the economy of the 21st century. Without a stable energy supply, health and welfare is threatened and the U.S. economy cannot function. More than 80 percent of the country's energy infrastructure is owned by the private sector.

The energy infrastructure is divided into three key segments: electricity, petroleum, and natural gas. These segments are interrelated (for example, natural gas is a key fuel for electricity production).

The U.S. electricity segment contains 5,000 power plants with approximately 905 gigawatts of generating capacity. Approximately 50 percent of electricity is produced by combusting coal, 20 percent in nuclear power plants, and 18 percent by combusting natural gas. The remaining generation is provided by hydroelectric plants (7%), oil (2%), and by renewable (solar, wind, geothermal) and other sources (3%). Electricity generated at power plants is transmitted over 158,000 miles of high-voltage transmission lines. Voltage is stepped down at more than 63,000 substations before being distributed to 131 million customers over millions of miles of lower voltage distribution lines. The electricity infrastructure is highly automated and controlled by utilities and regional grid operators using sophisticated supervisory control and data acquisition (SCADA) systems to keep the system in balance.

The petroleum segment entails the exploration, production, storage, transport, and refining of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors throughout the U.S. Key petroleum products include motor gasoline, jet fuel, distillate fuel oil, residual fuel oil, and liquefied petroleum gases. Both crude oil and petroleum products are imported, primarily by ship, as well as produced domestically. Currently 63 percent of the crude oil required to fuel the U.S. economy is imported. In the U.S. there are more than 500,000 crude oil producing wells, 30,000 miles of gathering pipeline and 74,000 miles of crude oil pipeline. There are 152 petroleum refineries, 95,000 miles of product pipeline, and 2,000 petroleum terminals. Petroleum also relies on sophisticated

SCADA and other systems to control production and distribution, but unlike electricity crude oil and petroleum products are stored in tank farms and other facilities.

Natural gas is also produced, piped, stored, and distributed in the U.S. Increasingly, natural gas is imported as liquefied natural gas (LNG). There are more than 383,000 gas production and condensate wells and 45,000 miles of gathering pipeline in the U.S. Gas is processed (impurities removed) at 726 gas processing plants, and there are over 254,000 miles of interstate pipeline for the transmission of natural gas. Gas is stored at 410 underground storage fields and 96 LNG storage facilities. Finally, natural gas is distributed to homes and businesses over 981,000 miles of distribution pipelines.

Sector Security Vision:

To ensure the continued viability of the U.S. economy and way of life, the Energy Sector will focus on protecting the assets essential to providing the reliable flow of energy to the American people, businesses and economy. The Energy Sector will collaborate with other critical infrastructure sectors and State and local governments to ensure that interdependencies are understood and addressed to ensure that critical operations are not interrupted should there be an energy sector disruption from natural or manmade sources.

F.9 Government Facilities Sector

The Government Facilities sector includes facilities are typically built, leased, or otherwise acquired to perform a specific departmental or agency mission at the Federal and State/local levels. A facility can consist of one building or multiple buildings on the same site. In many cases, it is important to note that such facilities serve as shells protecting mission-critical assets within.

All facilities fall into three basic categories:

- Domestic (non-defense): Domestic facilities are owned and managed by a Federal department or agency or by State, Territorial, or local government.
- Defense: Defense facilities are those owned and managed by the Department of Defense that do not fall under GSA or other specific department or agency management. Protective standards for military facilities are typically more stringent than those of the domestic facilities.
- Overseas: Overseas facilities are those located outside U.S. national borders. Security at these facilities is typically managed by the Overseas Security Policy Board, chaired by the National Security Council. Due to the higher threat environment of many overseas locations, these facilities utilize extremely stringent standards.

Sector Security Vision:

The Government Facilities Sector strives to prevent the damage or destruction of government owned or leased facilities that would result in the death or serious injury of tenants and the public. This will be accomplished through the use of innovative technology, deployment of trained law enforcement professionals and contract guards, and the adoption of building security programs, among other efforts. The Sector will encourage departments and agencies to achieve a higher sustainable level of awareness and vigilance.

F.10 Information Technology Sector

The Information Technology (IT) Sector produces hardware, software, and services that enable other sectors to function. For example, the IT Sector produces laptops, operating systems, and Internet search engines. These IT Sector products are consumed across other critical infrastructure sectors and the Government. The *production* of hardware, software, and services therefore comprises the IT Sector; the IT Sector may be considered as the “IT Industrial Base.”

The Internet is a key resource composed of assets within both the IT and Telecommunications Sectors and is used by all sectors in varying degrees of business and operational dependence. The availability of the service is the responsibility of the IT and Telecommunications Sectors, but the need for access to and reliance on, the Internet is common to all sectors.

Sector Security Vision:

The highly diverse IT Sector is committed to securing the IT infrastructure by being knowledgeable and adequately prepared to foresee attacks and, if possible, prevent attacks; and that the sector is robust enough to withstand attacks without incurring catastrophic damage;, responsive enough to recover from attacks in a timely manner; and, resilient enough to sustain nationally critical operations.

F.11 National Monuments and Icons Sector

The National Monuments and Icons (NM&I) Sector encompasses a diverse array of assets located throughout the U.S. and its territories. While many of these assets are listed in either the National Register of Historic Places or the List of National Historic Landmarks, all share three common characteristics: (1) they are a monument, physical structure, or geographic site; (2) they are widely recognized to represent the Nation's heritage, traditions, or values or widely recognized to represent important national cultural, religious, historical, or political significance; and (3) their primary purpose is to memorialize or represent some significant aspect of the Nation's heritage, tradition, or values, and to serve as points of interest for visitors and educational activities.

The NM&I Sector assets are all physical structures or geographic sites. Included as part of each asset are the operational staff and visitors that may be impacted by an attack on the asset. There are minimal cyber and telecommunications issues associated with this sector due to the nature of the assets. There may be some information technology or telecommunications systems utilized at a few of the assets, and these will be considered during the vulnerability assessment process and the protective program implementation as appropriate.

Some physical structures that could be considered as monuments or icons (e.g., Golden Gate Bridge, Sears Tower, Hoover Dam, and U.S. Capitol) have been determined to be more appropriately assigned to other sectors, such as transportation systems, commercial facilities, dams, and Government facilities, because of their primary purpose. NM&I SSP is primarily focused on the identification, assessment, prioritization, and protection of nationally significant NM&I that may be attractive terrorist targets.

Sector Security Vision:

The NM&I Sector is committed to ensuring that the symbols of our Nation remain protected and intact for future generations. In the course of protecting our landmarks, the Sector will ensure that staff and visitors are protected from harm. Because citizen access to these monuments and icons is a hallmark of life in a free and open society, the Sector will strive for an appropriate balance between security, public access, and aesthetics. The protective measures taken by the Sector will prevent adversaries from affecting the national psyche by damaging or destroying these important symbols.

F.12 Nuclear Reactors, Materials, and Waste Sector

Nuclear power accounts for approximately 20 percent of the Nation's electrical generating capacity. Nuclear power plants are among the best defended and most physically hardened of the CI/KR in the country, designed to withstand extreme events such as hurricanes, tornadoes, and earthquakes. Although losing the electrical generation of a single nuclear power plant might have only a minor impact on the Nation's overall electrical capacity, an event such as a terrorist attack would be considered a significant security event. In an unlikely scenario, a successful terrorist strike could result in a release of radioactive material.

Responsibility for coordination of the Commercial Nuclear Reactors, Materials, and Waste Sector was designated in HSPD-7 to DHS in close cooperation with, the Nuclear Regulatory Commission.

This Sector includes the Nation's 104 commercial nuclear reactors licensed to operate in 31 States. As noted in paragraph 29 of Homeland Security Presidential Directive-7 (HSPD-7), this Sector also includes non-power nuclear reactors used for research, testing, and training; nuclear materials (source, by-product, and special nuclear material) used in medical, industrial, and academic settings; nuclear fuel fabrication facilities; decommissioning reactors; and the transportation, storage, and disposal of nuclear materials and waste. Although some of these activities are not considered CI/KR by themselves, radioactive materials stolen from them could be used against other CI/KR.

This Sector has interdependencies with other sectors including the Energy Sector as a supplier to the Nation's electrical grid; the Transportation Systems Sector through the movement of radioactive materials; the Chemical Sector related to hazardous chemicals at fuel cycle facilities; the Public Health/Healthcare Sector through nuclear medicine, radiopharmaceuticals, and sterilization of surgical supplies; and the Government Facilities Sector through Federal and State facilities that use radioactive material for a myriad of purposes.

Sector Security Vision:

The Commercial Nuclear Reactors, Materials, and Waste Sector will support national security, public health and safety, public confidence and economic stability by enhancing, where necessary and reasonably achievable, its existing high level of readiness to promote the security of the sector's facilities; and to lead by example to improve the Nation's overall critical infrastructure readiness.

F.13 Postal and Shipping Sector

The Postal and Shipping Sector moves hundreds of millions of messages, products, and financial transactions each day. The Nation's economic and social processes rely on the ease and ubiquity of sending material to and from any location at optimal levels of speed and cost. Postal and shipping activity is differentiated from general cargo operations by its focus on small and medium-size packages and by service from millions of senders to millions of destinations. The sector is highly concentrated, with a handful of providers holding 95+ percent market share. But sector protection requires the involvement of more than just the delivery firms. Customers and other service firms are integrally involved in the value chain through the creation of sent items, work-sharing such as presort and drop-shipment, and mailroom operations. The web of sector providers, customers, and service firms extends internationally, posing important security challenges including customs inspection.

The sector shares activities and assets with the Transportation Sector, and the major postal and shipping providers operate nearly every mode of transportation. But there are also sector-specific assets including high-volume automated processing facilities; tens of thousands of local delivery units; many and varied collection, acceptance, and retail operations; mail transport equipment, such as trays and sacks; plus information and communications networks. Beyond these physical assets, the most critical sector asset is public trust. Faith in the security and safety of letters and packages is the foundation supporting sector activity.

The Postal and Shipping Sector relies on several sectors and is relied upon by others. The sector uses all transportation networks and the relationship is symbiotic, with mail being a major revenue source for commercial carriers. The Information Technology and Telecommunications Sectors are also critical—the distribution operations of major providers are based on automatic identification of pieces and their destination addresses. All industries rely on mail and shipping services, but none more so than financial services because of bill presentment/payments and the shipping of critical financial documents. Postal and shipping activity also poses a threat channel to other sectors. Delivery personnel often only need uniforms or branded vehicles to gain access to sensitive areas.

Sector Security Vision:

The vision of the Postal and Shipping Sector is to ensure continuity of operations and ease of use by creating a multi-layered security posture through effective collaboration between public and private sector security partners that denies terrorists the ability to exploit the sector, while preserving the public trust and supporting the Nation's economy.

F.14 Public Health and Healthcare Sector

The Public Health/Healthcare Sector consists of State and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles. As technology has advanced, so has the level of integration of cyber within the sector (e.g., electronic record keeping systems). The U.S. also depends on several highly specialized laboratory facilities and assets, especially those related to disease control and vaccine development and storage, such as the Centers for Disease Control and Prevention, the National Institutes of Health, and the Strategic National Stockpile.

The Public Health and Healthcare Sector is highly decentralized and loosely coupled. Elements of this sector are present in virtually all U.S. communities. The Department of Health and Human Services, as the designated Federal agency responsible for coordinating efforts of the sector, will work with sector security partners to minimize vulnerabilities to physical security threats. The sector is also becoming more interconnected electronically, spurred by market forces, increasing information technology capabilities, a growing appreciation for the promise of information technology in improving efficiency and effectiveness, and a variety of Federal, State, local, and private-sector initiatives. Suppliers, payers, service providers, and patients are moving toward broader information exchanges. Attendant to these advancements is a growing set of potential information technology vulnerabilities.

Elements of the Public Health/Healthcare sector respond to nearly all conceivable attacks or related disasters. In a significant disaster or emergency, the U.S. population will depend on Public Health/Healthcare capabilities and stockpiles. Protecting the sector against threats and mitigating their effects, both physical and cyber, will help ensure continuity of patient care in the event of an emergency. In times of military conflict, the various groups compete for the same supplies, in some cases from the same sources (e.g., blood, blood products, and surgical supplies). This competition for resources can sometimes affect the ability of the civilian sector to care for the public even without a national disaster.

Sector Security Vision:

The Healthcare and Public Health Sector strives to prevent damage to, or destruction of, the Nation's healthcare and public health infrastructure with a view maintaining its functional integrity for timely and effective responses to both routine and emergency situations. Additionally, the sector is committed to protecting its workforce from harm resulting from terrorist or criminal activities, and epidemics to the extent possible.

F.15 Telecommunications Sector

Over the past 20 years, the Telecommunications Sector has evolved from predominantly a provider of equipment and voice services into a diverse, competitive, and interconnected industry. Although market competition and network convergence have helped lower prices and spur the development of new services, the Sector faces new challenges in protecting critical telecommunications assets for homeland security purposes.

The private sector is, and will remain, responsible for protecting the telecommunications infrastructure and assets. The industry has a proven track record for securing physical facilities and networks from natural or manmade threats and for restoring services in the aftermath of attacks. Working with the Federal Government, the private sector is able to predict, anticipate, and respond to sector outages and to

understand how they might affect the ability of the national leadership to communicate during times of crisis, impact the operations of other infrastructures, and affect response and recovery efforts. The telecommunications sector can be identified within three broad components:

- Wireline: The wireline component primarily consists of the public switched telephone network (PSTN), but also includes cable networks and enterprise networks. The PSTN is a domestic telecommunications network accessed by telephones, key telephone systems, private branch exchange (PBX) trunks, and data arrangements. Completion of the circuit between the call originator and the call receiver requires network signaling in the form of dial pulses or multi-frequency tones. These components are connected by nearly two billion miles of fiber and copper cable (physical), dedicated staff to ensure service (people), and information technology (IT) systems that monitor and move the data (cyber). Despite the industry's transition to packet-based networks, the traditional PSTN still remains the backbone of the telecommunications infrastructure.
- Wireless: Wireless communications include cellular telephone, paging, personal communications services, high-frequency radio, and other commercial and private radio services. Mobile wireless services, such as Cingular, T-Mobile, and Verizon Wireless, have become indispensable for businesses and consumers, as well as for public safety needs. According to industry estimates, the U.S. mobile market exceeded 50 percent of the population in 2003, with market penetration reaching almost 70 percent in the largest metropolitan markets.
- Satellite: Satellite communication systems use a combination of terrestrial and space components to deliver various telecommunications, Internet data, and video services. Geostationary Earth Orbit (GEO) systems typically require three satellites to have a global footprint. Non-geostationary-Low Earth Orbit (LEO) and Middle Earth Orbit (MEO) systems require numerous satellites for global coverage. A group of satellites working in concert is known as a satellite constellation.

Sector Security Vision:

The Telecommunications Sector acknowledges the Nation's critical reliance on assured communications and will strive to ensure the Nation's communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster.

F.16 Transportation Sector

The Nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas. The transportation system directly employs one of every eight members of the U.S. labor force and accounts for approximately eight percent of the gross domestic product. Because this system is so diverse and expansive, security risks are inherent in both the supporting infrastructure and the people and products moving through it. The global nature of this commerce, coupled with the global threat of terrorism, requires the U.S. to cast a security net that extends well beyond the point-of-entry of those goods and people. To be successful in this effort, coordination is required to gather and share critical information (including best practices) with the private sector, the international community, and the domestic and foreign agencies responsible for the protection of transportation assets.

The Transportation Sector consists of six key subsectors, or modes:

- Aviation includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional airfields. Additionally, this mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.
- Highway encompasses more than four million miles of roadways and supporting infrastructure (bridges, tunnels, interchanges, traffic management centers, terminals, transfer points, and facilities). Vehicles include cars, buses, motorcycles, and all kinds of trucks.

- Maritime includes vessels, ports, inland waterways, harbors, navigable waters, the Great Lakes, territorial seas, contiguous waters, customs waters, coastal seas, littoral areas, as well as sea-lanes and maritime approaches to the U.S..
- Mass Transit includes multiple-occupancy vehicles, such as transit buses, trolleybuses, vanpools, monorails, heavy (subway) and light rail, automated guideway transit, inclined planes, and cable cars, designed to transport customers on local and regional routes.
- Pipeline Systems includes vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the Nation's natural gas and about 65 percent of hazardous liquids (crude and refined oil products).
- Rail consists of hundreds of railroads, more than 143,000 route miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives. Amtrak operates over more than 22,000 route miles in 46 States and Washington, D.C., and has some 500 station stops.

The Transportation Sector has significant interdependencies with the majority of the other critical infrastructure sectors. For instance, the Transportation and Energy Sectors directly depend on each other—to move vast quantities of fuel to a broad range of users and to supply the fuel for all sorts of transportation. In addition to cross-sector interdependencies, the Transportation Sector must also deal with interdependencies among modes.

Sector Security Vision:

Our vision is a secure and resilient transportation network, enabling legitimate travelers and goods to move safely and efficiently, from point of origin to destination, without undue fear of harm or catastrophic disruption of service, affirming economic vitality and public confidence through a layered defense of best security practices.

F.17 Water Sector

The Water Sector includes both drinking water and wastewater (Water Sector) utilities. The sector is vulnerable to a variety of attacks through contamination with deadly agents, the release of toxic gaseous chemicals, and other means that could result in thousands of casualties, and/or the loss of water to support economic activity, fire fighting, and other critical services. There are approximately 160,000 public water systems (PWS) in the U.S. These PWS serve 84 percent of the U.S. population. Wastewater is treated by publicly owned treatment works (POTWs) and by private facilities such as industrial plants. There are more than 16,000 POTWs that serve 75 percent of the U.S. population.

Even before the Environmental Protection Agency (EPA) was designated in HSPD-7 as the agency responsible for coordinating Water sector efforts, many of their ongoing programs supported security-related activities. In addition, the Public Health Security and Bioterrorism Preparedness and Response Act (Bioterrorism Act) provides explicit authority regarding community water systems. This Act requires community drinking water systems serving populations of more than 3,300 persons to conduct vulnerability assessments (VAs) and prepare or upgrade emergency response plans based on the finding of their VAs. Since the passage of this Act, it became apparent that a broad-based strategy was required to address the security needs of the entire water sector as reflected by the promulgation of HSPD-7. This strategy is comprised of four key initiatives: risk identification; protection and preparedness; response, recovery, and decontamination; and research. The work includes providing support to utilities by preparing vulnerability assessment and emergency response tools, providing technical and financial assistance, and information exchange.

Sector Security Vision:

To better secure the Nation's critical drinking water and wastewater infrastructures, the Water Sector will focus on having security programs in place that enhance its ability to prevent, detect, respond to, and recover from potential terrorist or other intentional acts. These efforts will assist in ensuring the safety of the Nation's drinking water supply and the protection of water quality by reducing the risk to public health, the environment, and critical infrastructure.

Appendix G: Recommended Homeland Security Practices for use by the Private Sector

This appendix provides a summary of practices that may be adopted by private sector owners and operators to improve the efficiency and effectiveness of their CI/KR protective measures. The recommendations are based on "best practices" currently in use by various sectors and groups. The NIPP encourages private sector owners and operators to adopt and implement those practices that are appropriate and applicable for the specific sector and individual organization:

Asset Identification

- Implement the NIPP framework for the assets under their control; and
- Provide CI/KR related data to DHS to facilitate national protection program implementation;

Risk/Vulnerability

- Conduct appropriate risk and vulnerability assessment activities using tools or methods accepted as industry standard, or in case of physical vulnerabilities, endorsed by the Department of Homeland Security;
- Implement appropriate risk mitigation and emergency programs;
- Evaluate vulnerabilities of suppliers and customers that may significantly affect owners or operators and take appropriate action;
- Implement measures to reduce risk and eliminate deficiencies and vulnerabilities in the cyber, physical, and people security controls;
- Maintain the tools, capabilities, and protocols to provide an appropriate level of monitoring of the facility and its immediate surroundings to detect possible insider and external threats;
- Screen employees and suppliers working in sensitive positions through the use of background checks; and
- Manage the security of computer systems while maintaining awareness of vulnerabilities and consequences to ensure that systems are not used to enable attacks against CI/KR.

Information Sharing

- Connect with, and participate in, the appropriate local, regional, national, and sector information-sharing mechanisms;
- Develop and maintain working relationships with local (and, as appropriate, State, Territorial, tribal, and Federal) law enforcement and first responder organizations relevant to the company's facilities to promote communication and cooperation related to prevention, remediation and response to a natural disaster or terrorist event. Prepare and post contact lists for company and Government emergency contacts in a prominent location in all Departments and ensure that all personnel are familiar with communications mechanisms for first responder and State and Federal Homeland Security officials;
- Provide information on threats, assets, and vulnerabilities to appropriate government authorities;
- Share threat and other appropriate information with other owners and operators;
- Participate in NIPP Sector Coordinating Council activities;
- Participate in and support State and local CI/KR protection programs;
- Collaborate with infrastructure owners and operators on issues of mutual concern;

- Evaluate security threats or incidents including possible surveillance, respond to the incidents and, if warranted and appropriate, report them to law enforcement personnel and/or State, Territorial, and Federal Homeland Security officials; and
- Use appropriate measures to safeguard information that would pose a threat in the wrong hands. Maintain open and effective communications regarding security measures and issues, as appropriate, with employees, suppliers, customers, government officials, and others.

Planning and Awareness

- Review and implement appropriate provisions of the National Fire Protection Association (NFPA) 1600, Standard on Disaster/Emergency Management and Business Continuity Programs, endorsed by DHS and the American National Standards Institute (ANSI);
- Participate in exercises and other activities to enhance individual and sector preparedness;
- Demonstrate a robust governance capability through its commitment to security and resiliency across the entire company;
- Develop a mitigation strategy and execution plan with an achievable timeframe;
- Develop and communicate an acceptable plan and protocol for each of the levels of the Homeland Security Advisory System. These plans and protocols are additive so that as the threat level increases for company facilities, the company can quickly implement its plans to enhance cyber or physical security measures in operation at those facilities;
- Develop and implement both Business Continuity Plans and Disaster Recovery Plans to allow the business to survive and respond to a major natural disaster or terrorist event. These plans provide for physical displacement of the business and all associated human and technology infrastructure for the short term (less than one month) and long term (more than 1 month);
- Document the key elements of security programs, actions and periodic reviews as part of a commitment to sustain a consistent, reliable, and comprehensive program over time;
- Enhance security awareness and capabilities through periodic training, drills and guidance that involve all employees annually to some extent and, when appropriate, involve others such as emergency response agencies;
- Conduct periodic third-party audits to measure the effectiveness of its planned physical and cybersecurity measures. These audits and verifications are reported directly to the Chief Executive Officer or the Chief Executive's designee for review and action;
- Promote emergency response training such as the Community Emergency Response Team training offered by the U.S. Citizen Corps, for employees; and
- Consider including programs for developing highly secure and trustworthy operating systems in near-term R&D priorities.

Appendix H: International Coordination

H.1 Introduction and Purpose of this Appendix

This appendix provides guidance for addressing the international aspects of CI/KR protection in support of the NIPP.

H.1.1 Scope

The NIPP provides the mechanisms, processes, key initiatives and milestones required for the Department of Homeland Security, the Department of State, SSAs and other security partners to address international implications and requirements related to CI/KR protection. The NIPP and associated SSPs recognize that protective measures do not stop at a facility's fence line or a national l border. Because disruptions in the global infrastructure can ripple and cascade around the world, the NIPP and SSPs also must consider trans-border infrastructure, international vulnerabilities, and global and sector dependencies and interdependencies.

H.1.2 Vision

The *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* identifies "fostering international cooperation" as one of the eight guiding principles of its vision for the future. The strategy underscores the need for a coordinated, comprehensive, and aggressive global action as a key aspect of the NIPP approach to CI/KR protection.

Furthermore, the *National Strategy to Secure Cyberspace* set forth strategic objectives for National Security and International Cyberspace Security Cooperation that deal directly with the international aspects of CI/KR protection including the prevention of cyber attacks against America's critical infrastructure, reducing vulnerabilities, and minimizing damages and recovery time from cyber attacks that do occur.

H.1.3 Implementing the Vision with a Strategy for Effective Cooperation

The NIPP CI/KR international coordination and protection strategy outlined in this appendix is focused on instituting effective *cooperation with international security partners*, rather than on *specific protective measures*. Specific protection measures are tailored to each sector's particular circumstance and are developed in Sector-Specific Plans. This appendix also focuses on implementing existing agreements that affect CI/KR protection and on addressing cross-sector and global issues such as cybersecurity.

Within six months of the approval of the NIPP, DHS, the Department of State, and other concerned Federal agencies will incorporate the NIPP into their strategies for cooperating with other countries and international organizations. The broad structure of this strategy is outlined in this appendix; it is based on the following high-level considerations.

H.2 Responsibilities for International Cooperation on CI/KR Protection

In accordance with HSPD-7, the Department of State, in conjunction with DHS, the Departments of Justice, Commerce, Defense, the Treasury, and other appropriate agencies, is responsible for working with foreign countries and international organizations to strengthen the protection of U.S. CI/KR. This section provides further details regarding the responsibilities of DHS and other security partners relating to the international dimension of CI/KR protection.

H.2.1 Department of Homeland Security

DHS is responsible for coordinating the overall national effort to enhance the protection of U.S. CI/KR, and has specific responsibility for the information technology, telecommunications, chemical, transportation systems, emergency services, postal and shipping, dams, government facilities, and commercial facilities sectors.

Under the CI/KR risk management framework described in this Plan, DHS is responsible for the following actions, all of which have an international dimension:

- Building security partnerships;
- Implementing a comprehensive, integrated risk management program; and
- Implementing protective programs.

DHS, in conjunction with the Department of State, will share with international entities appropriate information and perform outreach functions to enhance information sharing and management of international agreements regarding CI/KR protection.

Some of the more complex challenges presented by the international aspects of CI/KR protection involve analyzing the complex dependencies, interdependencies, and vulnerabilities that require the application of sophisticated and innovative modeling techniques to assess. DHS is responsible for pursuing research and analysis in this area. It will call on a range of outside sources for this work including those with expertise in the international community and the National Infrastructure Simulation and Analysis Center (NISAC).

H.2.2 Department of State

The Secretary of State has direct responsibility for policies and activities related to the protection of U.S. citizens and U.S. facilities abroad. The Secretary of State, in conjunction with the Secretary of Homeland Security, is responsible for coordinating with foreign countries and international organizations to strengthen the protection of U.S. CI/KR. The Department of State supports DHS and other Federal agency efforts by providing knowledge about and access to other governments. The Department of State leverages bilateral and multilateral relationships around the world to ensure that the U.S. Government can act effectively in identifying and protecting U.S. CI/KR.

The Department of State, DHS, and other agencies are engaged in a wide range of activities throughout the world to prevent, disrupt, and deter threats and acts of terrorism directed against the homeland and U.S. interests abroad. The objectives of these efforts are to develop and work with global partners to ensure mutual security and to raise awareness of the terrorist threat.

H.2.3 Other Federal Agencies

SSAs exchange information, including cyber-specific information, with security partners in international community, in accordance with guidelines established by DHS and Department of State and as appropriate to improve the Nation's overall CI/KR protection posture.

The Departments of Justice, Commerce, Defense, Treasury, and other Departments share responsibility, in accordance with HSPD-7, for working with foreign countries and international organizations to strengthen the protection of U.S. CI/KR.

H.2.4 State, Territorial, Tribal, and Local Governments

State and Territorial governments ensure ongoing cooperation with relevant international, regional, local and private sector CI/KR protection efforts.

H.2.5 Private Sector

DHS is working with the private sector, SSAs, and information-sharing mechanisms and organizations to protect trans-border infrastructure and understand international and global vulnerabilities. DHS relies on the private sector for data, expertise and knowledge of their international operations to identify relevant international assets and assess risks.

H.2.6 Academia

The academic community provides data, insight, and research into the significance of international interdependencies, modeling and analysis, and uncovers previously unknown nodes, behaviors and vulnerabilities.

H.3 Managing the International Dimension of CI/KR Risk

The NIPP addresses international CI/KR protection, including interdependencies and the vulnerability to threats that originate outside the country. The NIPP brings a new focus to international security cooperation, and provides a risk–based strategic framework for measuring the effectiveness of international CI/KR protection activities. The NIPP also provides tools to assess international vulnerabilities and interdependencies that complement long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides a framework for effective collaborative engagement with additional international partners.

SSPs are required to include international considerations as an integral part of each sector's planning process rather than instituting a separate layer of planning. Some international aspects of CI/KR protection require additional overarching or cross-sector emphasis. These include:

- U.S. interaction with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructures that often have an international or even global dimension;
- Protection of physical assets located on or near the borders with Canada and Mexico that requires cooperation with and/or planning and resource allocation among neighboring countries, States bordering on these countries and affected tribal and local governments;
- Sectors with infrastructure that is extensively integrated into an international or global market (e.g., financial services or other information-based business, energy, or transportation) or when the proper functioning of a sector relies on inputs that are not within the control of U.S. entities; and
- U.S. Government and corporate facilities located overseas that may be regarded as CI/KR. Protection for the Government Facility Sector involves careful *interagency* cooperation as well as cooperation with for foreign CI/KR security partners.

The following sub-sections discuss issues associated with the international aspects of CI/KR protection in the context of the steps of the NIPP risk management process. (See NIPP Chapter 3: The Protection Program Strategy: Reducing Risk).

H.3.1 Setting Security Goals

The overarching goal of the NIPP—to enhance the Nation's protection of U.S. CI/KR—applies to the international system of systems that underpins U.S. CI/KR. The NIPP and the SSPs provide goals and protective actions that address the international aspects of CI/KR protection effort on a sector-specific basis. In addition, a separate set of goals and priorities guide cross-sector efforts to improve protection for CI/KR with international linkages. These goals fall in three categories:

- Identifying and addressing cross-sector and global issues;
- Implementing existing and developing new agreements that affect CI/KR; and
- Improving the effectiveness of international cooperation.

DHS, in conjunction with the Department of State and other security partners, will define a comprehensive international CI/KR protection strategy for pursuing and achieving these goals in ways that complement each other and are achievable with the resources available.

Important considerations in achieving these goals are discussed in this section; actions required to achieve these goals are addressed in the section on key implementation actions below.

H.3.2 Identifying Assets Affected by International Linkages

Once international security goals are set, the next step in the risk management process is to develop and maintain a comprehensive inventory of the Nation's CI/KR outside the U.S. borders and of foreign CI/KR that may affect systems within this country. The process for identifying nationally critical assets involves working with U.S. industry, SSAs, academia and international partners to gather information on the foreign infrastructure and resources on which U.S. CI/KR relies.

H.3.2.1 Dependency and Interdependency and International CI/KR Protection Cooperation

The NIPP risk management framework details a structured approach to use when determining dependencies and interdependencies, including physical, cyber and international. This approached is designed to address CI/KR protection in three areas:

1. Direct international linkages to physical and cyber U.S. CI/KR:
    - Foreign trans-border assets linked to U.S. CI/KR such as roads, bridges, pipelines, gas lines, power lines etc. physically connecting U.S. CI/KR to Canada and Mexico;
    - Foreign infrastructure whose disruption or destruction could directly harm the U.S. homeland such as waters behind a Canadian dam that could flood U.S. territory and a toxic plume from a destroyed Mexican chemical plant that could contaminate U.S. territory; and
    - U.S. CI/KR that may be located overseas such as non-military government facilities; overseas component of U.S. CI/KR.
2. Indirect international linkages to physical and cyber U.S. CI/KR:
    - The potential, cascading, and escalating effects of disruption or destruction of foreign assets, networks and systems, critical foreign technology, goods, resources, transit routes, and chokepoints; and
    - Foreign ownership, control, or involvement in U.S. CI/KR and related issues.
3. Global aspects of physical and cyber U.S. CI/KR
    - Infrastructure assets either located around the world or with global mobility, and that require the efforts of multiple foreign countries to secure.

Dependency and interdependency analysis is primarily based on information from each sector and is informed by the judgments of CI/KR owners and operators regarding their supply chains and sources of other services from other infrastructure sectors such as power and water. As the capability for sophisticated network analysis grows, these inputs will be complemented by assessments that examine less apparent network-based dependencies and interdependencies. The National Infrastructure Simulation and Analysis Center (NISAC) supports this effort by analyzing and quantifying national and international dependency and interdependency for complex systems that affect specific sectors.

H.3.3 Assessing Risks

The risk assessment for CI/KR assets and systems that are affected by international linkages is an integral part of the risk management framework described in the NIPP. The risk management framework combines consequences, threats, and vulnerabilities to produce systematic, comprehensive, and risk assessments that can be clearly explained in a three-step process:

1. Determining the consequences of destruction, incapacitation, or exploitation of an asset. This is done to assess potential national significance as well as physical, human, and cyber dependencies and interdependencies that may result from international linkages need to be assessed.
2. Analyzing vulnerability including determining which elements of infrastructure are most susceptible to attack and whether attacks against these elements could be a consequence of any international linkages; and
3. Conducting a threat analysis that provides the likelihood that a target will be attacked. CI/KR with international linkages may present greater opportunities for attack and thus increase the likelihood that they may be the subject of attacks.

H.3.4 Prioritizing

Assessing assets on a level playing field that adjudicates risk based on a common framework ensures that resources are applied where they offer the most benefit for reducing risk, deterring threats, and minimizing the consequences of attacks. The same prioritization disciplined used for domestic CI/KR protection is observed to evaluate the risk arising from international linkages. The priority for protection investments could be raised if international linkages increase the risk.

H.3.5 Implementing Programs

The SSAs have primary responsibility for developing protective measures that address risks that arise from international factors. In addition to sector protective measures, DHS has specific programs to help enhance the cooperation and coordination needed to address the unique challenges posed by the international aspects of CI/KR protection:

- **International outreach program:** DHS works with the Department of State to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructures on which the United States depends.
- **The National Cyber Response Coordination Group:** The National Cyber Response Coordination Group (NCRCG) facilitates coordination of the Federal Government's efforts to prepare for, respond to and recover from cyber Incidents of National Significance and other National cyber incidents and physical attacks that have significant cyber consequences (hereinafter collectively "Cyber Incidents'). It serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber crisis. During such incidents, NCRCG member-agencies integrate their capabilities to assess the domestic and international scope and severity of a cyber incident.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the "steady-state" protection plans and programs put in place by the NIPP. The exercise program, as appropriate, engages international partners to address cooperation and cross-border issues including those relating to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners.
- **National Cyber Exercises:** DHS is conducting exercises to identify, test, and improve coordination of the cyber incident response community, to include Federal, State, Territorial, tribal, local, and international government elements as well as private sector corporations and coordinating councils.

Because of the nature of the international dimension of CI/KR a substantial emphasis is placed on standards that can be used to improve cooperation and coordination. To this end DHS will lead efforts to:

- Collaborate to establish global standards successful protection measures or best practices relating to telecommunications, air transportation systems, container shipping, cybersecurity, and other global systems as appropriate.
- Encourage the development of ISO-like standards and related agreements that can help to reduce insurance premiums and level CI/KR protection costs for businesses.

H.3.6 Measuring Effectiveness and Making Improvements

The NIPP specifies three types of quantitative indicators to measure program effectiveness:

- Descriptive metrics that are necessary to understand sector resources and activity; they do not reflect CI/KR protection performance;
- Process metrics measure whether specific activities were performed as planned; these track the progression of a task or report on the completion of an enabling process such as forming a bilateral partnership; and
- Outcome metrics track progress towards a strategic goal by beneficial results rather than level of activity.

The NIPP also distinguishes between two groups of metrics: core metrics that enable comparison and analysis between and among different sectors and sector-specific metrics that are useful within a sector.

Because protective measures are designed, implemented, and evaluated through sector specific mechanisms guided by the SSPs, they deal with the protection challenges for a particular facility, network or sector rather than international issues that may affect protection measures. Conversely, most initiatives that address the international issues affecting CI/KR protection are enablers rather than protective measures themselves. As a result, the metrics used to measure the effectiveness of international CI/KR protection initiatives will primarily be process metrics in the core group of CI/KR protection metrics. These will measure progress on tasks that enable CI/KR protection in situations that have international ramifications.

These metrics will be used to manage the comprehensive international CI/KR protection strategy, which enables SSP protection initiatives, and to track progress toward the strategy's three goals:

- Improving the effectiveness of international cooperation;
- Implementing existing and developing new agreements that affect CI/KR; and
- Addressing cross-sector and global issues.

DHS will develop the metrics to track progress on international CI/KR protection enablers. Examples of such metrics include:

- The international issues being faced by each sector, which of these affect multiple sectors and which issues are the most important;
- The countries that should be involved in protection partnerships for each sector;
- The number and type of bilateral and multinational agreements affecting CI/KR protection;
- The nature, level of implementation, and effectiveness of bilateral and multinational agreements;
- The sectors affected by each international partnership;
- The number and type of outcomes enabled by an international initiative; and
- Where possible, the specific CI/KR protection enhancements that are directly attributable to a particular international initiative.

Once the core metrics have been developed and approved, DHS and its relevant security partners will establish a data-gathering and reporting process. This process will outline, but will not be limited to, responsibilities, data collection and reporting procedures and timeframes, metrics calculation, and the schedule for computing and updating the metrics on a regular basis.

H.4 Organizing International CI/KR Protection Cooperation

DHS, in conjunction with the Department of State and other Federal agencies, works with individual foreign governments, and regional and international organizations in partnership to enhance the protection of the Nation's CI/KR and to deny the exploitation of CI/KR assets. Potential partnerships depend on:

- Physical proximity to the United States or U.S. assets;
- Useful experience, information to be gained from other countries;
- Existing alliances and agreements, and high-level commitments;
- Critical supply chains and vulnerable nodes; and
- Interdependencies and networked technologies, and the need for a global "culture of security" to protect physical and cyber assets.

As international CI/KR protection partnerships mature, cooperative efforts will strengthen in two dimensions:

- Development of new partnerships with countries possessing useful experience and information regarding CI/KR protective efforts, as well as terrorism prevention, preparedness, response and recovery;
- Development of new international relations and institutions to protect global infrastructures and to address international interdependencies, networked technologies and the need for a global culture of security to protect physical and cyber assets.

The coordination mechanisms supporting the NIPP create linkages between CI/KR protection efforts at the national, sector, State, Territorial, local, tribal, regional, and international levels. The organizations and bodies that are involved with this coordination are diverse and depend on the specifics of the issues they address and other considerations as discussed in the following subsections.

H.4.1 Domestic Aspects of International CI/KR Protection Cooperation

H.4.1.1 Interagency Coordination –Department of State and DHS Leadership

DHS will work with the Department of State, international partners, and with U.S. entities involved with the international aspects of CI/KR protection, to exchange experiences, share information and develop a cooperative atmosphere to materially improve U.S. critical infrastructure protection, information sharing, cybersecurity, and global telecommunications standards. DHS and SSAs will work with specific countries to identify international interdependencies and vulnerabilities. SSAs will consider such international factors as trans-border infrastructure, international vulnerabilities, and global interdependencies in their SSPs.

H.4.1.2 Interagency Coordination–Review of Existing Mechanisms to Support the NIPP

The International Affairs offices in U.S. Government agencies maintain existing relationships with foreign counterpart ministries and agencies, and are the primary partners with Department of State in coordinating with foreign governments on international CI/KR matters.

DHS also works with SSAs to ensure that SSPs reflect international factors such as trans-border infrastructure, international interdependencies, and global vulnerabilities.

The Department of State presently chairs an interagency working group that coordinates U.S. international CI/KR protection outreach activities. Within 30 days of publication of this Plan, the Department of State and DHS will review the working group's charter and its coordination mechanisms to ensure they address all international CI/KR issues specified by the NIPP. The Department of State and DHS will, within an additional 30 days, implement any changes that are needed to ensure that all NIPP requirements will be met and that the working group's charter reflects a role that best supports the comprehensive international CI/KR protection strategy.

H.4.1.3 Regional Coordination

U.S. regional initiatives can include public-private partnerships that cross international boundaries and focus on preparedness within a defined geographic area. These initiatives are unique to the geography, security partners, and sector interests. The National Homeland Security Regional Initiative provides a channel for information-sharing between U.S. regional initiatives with an international dimension and DHS.

H.4.2 Foreign Aspects of International CI/KR Protection

International cooperation on cybersecurity and other CI/KR protection issues of a global nature is necessary because of the trans-border or borderless nature of these infrastructures. These efforts require interaction on both the policy and the operational levels and involve a broad range of entities from both the government and the private sector. Interaction on the international aspects of CI/KR protection takes place bilaterally, regionally, and multilaterally:

- **Bilateral:** DHS participates in bilateral discussions and programs with countries of interest where there are issues that can best addressed on a country-to-country basis.
- **Regional:** DHS also provides leadership in regional groups, such as the Organization of American States (OAS) and the Asia Pacific Economic Cooperation (APEC), to raise awareness and develop cooperative programs.

  The United States engages with Canada and Mexico, as regional neighbors, on critical infrastructure protection to enhance collaboration efforts. Current activities include the U.S., Canada and Mexico trilateral Security and Prosperity Partnership; the U.S.-Canada Critical Infrastructure Protection Framework for Cooperation (Smart Border Action Plan) and the U.S.-Mexico Critical Infrastructure Protection Framework for Cooperation (Border Partnership Action Plan).
- **Multilateral:** Multilateral collaboration on this aspect of CI/KR involves initiatives on the part of the Organisation for Economic Cooperation and Development (OECD), G8, and United Nations. For the cybersecurity aspects of global CI/KR protection, DHS has established a preliminary framework for cooperation on cybersecurity policy, watch and warning, and incident response for CI/KR with key allies such as the Australia, Canada, New Zealand, and the United Kingdom. DHS is coordinating and participating in the establishment of an International Watch and Warning Network (IWWN) among cybersecurity policy, computer emergency response, and law enforcement participants of 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build cyber situational awareness and coordinate incident response.

H.4.3 Working with Specific Countries and International Organizations

DHS, SSAs and other security partners will work with other countries to promote CI/KR protection standards and best practices and it will pursue infrastructure security through international organizations such as the G8, NATO, the European Union, the Organization of American States and the Organisation for Economic Cooperation and Development. The approach to working with some specific countries and organizations is founded on formal agreements that address cooperation on CI/KR protection.

- **Canada and Mexico:** The CI/KR relations between the United States and its immediate neighbors make the borders virtually transparent. Electricity, natural gas, oil, roads, rail, food, water, minerals and finished products flow both ways across the borders. The importance of this trade, and the infrastructures that support it, was highlighted after the terrorist attacks of September 11, 2001 nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and 2002 Border Partnership Declaration with Mexico in part to address bilateral CI/KR issues. In addition, the 2005 Security and Prosperity Partnership of North America (SPP) established a trilateral approach to common security issues. The SPP is based on the principle that the prosperity of all three Nations is dependent on mutual security. The SPP complements, rather than replaces existing agreements.

- **United Kingdom:** The United Kingdom is a close ally with long experience in fighting terrorism and protecting its CI/KR. The United Kingdom has developed law enforcement and intelligence systems, and protection of the commercial facilities sector. Like the United States, most of the critical infrastructure in the United Kingdom is under private management. The U.K. Government has developed an effective, sophisticated system of managing public-private partnerships. DHS has formed a Joint Contact Group with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.

- **G8:** In the terrorist attacks against the United States, Spain, the United Kingdom, the infrastructures in G8 countries were exploited and used to inflict casualties and fear. The G8 has underscored its determination to combat all forms of terrorism and to strengthen international cooperation. Counter terrorism work has been the focus of a number of initiatives launched at recent summits. At their meeting in Glen Eagles in July 2005 the G8 heads of government issued a Statement on Counter-Terrorism (http://www.g8.gov.uk). In it they pledged to "commit ourselves to new joint efforts. We will work to improve the sharing of information on the movement of terrorists across international borders, to assess and address the threat to the transportation infrastructure, and to promote best practices for rail and metro security." DHS will work closely with the G8 to address the common threats to CI/KR and cyberspace.

- **European Union:** Following the 2004 terrorist bombings in Madrid, Spain, the European Union seriously addressed the problem of protecting interdependent CI/KR in open societies. The EU is pursuing CI/KR as a matter of policy, noting that an effective strategy should focus on both preparedness and on consequence management. DHS will engage the EU early in this process to share its experience, and to further cooperate on characteristics and common vulnerabilities of critical infrastructure and cyberspace, risk analysis techniques and strategies to reduce risk and minimize consequences.

- **NATO:** NATO addresses CI/KR issues through the Senior Civil Emergency Planning Committee (SCEPC) and has developed considerable expertise in coordination, logistics, and response. DHS has a delegation to SCEPCE at NATO, participates in NATO's telecommunications working group, and engages with NATO in preparedness exercises.

H.4.4 Foreign Investment in U.S. CI/KR

Infrastructure protection may be affected by foreign investment and ownership of sector assets. At the Federal level, this issue is monitored by the Committee on Foreign Investment in the United States (CFIUS) and in some cases the Federal Communications Commission. In February 2003, the Department of Homeland Security was added to CFIUS. The council also includes the Secretaries of State, Defense, and Commerce; the Attorney General, the Director of the Office of Management and Budget; the U.S. Trade Representative, and the Chairman of the Council of Economic Advisers, and is chaired by the Secretary of the Treasury.

DHS has important responsibilities on these government commissions that support the NIPP. These include:

- As a member of the Committee on Foreign Investments, DHS performs an examination of the impact of proposed foreign investments on CI/KR protection. The committee coordinates the development and negotiation of security agreements with foreign entities that may be necessary to manage the risk to CI/KR that a foreign investment may pose. DHS leads Government monitoring activities aimed at ensuring compliance with these agreements.
- DHS acts as a partner with the Department of Justice in supporting executive branch reviews of applications to the Federal Communications Commission from foreign entities pursuant to section 214 of the Communications Act of 1934 to assess if they pose any threat to CI/KR protection.

H.4.5 Information Sharing

Effective international cooperation of CI/KR protection requires a system for information sharing that includes process and protocols for updates among all partners, mechanisms for systematic sharing of best practices, and frequent opportunities for partners to meet to discuss and address international CI/KR issues.

The Homeland Security Operations Center (HSOC) serves as the Nation's hub for information sharing, situational awareness for domestic incident management—increasing coordination among with those members of the international community that are involved because of the role they play in protecting U.S. CI/KR.

The Homeland Security Information Network supports ongoing information-sharing efforts by offering Communities of Interest for selected international partners requiring close coordination with the HSOC.

DHS also provides mechanisms such as the DHS Cyber Portal to improve information sharing and coordination among government communities and selected international security partners for cybersecurity. The Cybercop Portal is a secure Internet-based information sharing mechanism for law enforcement members involved in the field of electronic crimes investigations. This secure, Internet based collaborative tool links and supports the law enforcement and investigative community worldwide serving participants from more than 40 countries.

H.5 Integration with Other Plans

The NIPP brings a new focus to the international security cooperation, and provides a risk–based strategic framework for measuring the effectiveness of international activities. The NIPP processes serve as management tools to assess international vulnerabilities and interdependencies. The NIPP process complements long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others and provides the framework for collaborative engagement with additional international partners.

SSPs are required to include a description of sector relationships, as well as roles and responsibilities of security partners that include international organizations and foreign countries. They are also required to take a comprehensive, integrated view of the asset to include the characteristics, dependencies, and interdependencies; international links; and cyber systems needed for it to function.

H.6 Ensuring International Cooperation Over the Long Term

The effort to ensure a sustainable approach to addressing the international aspects of CI/KR protection over the long term requires special consideration in the following areas:

- **Awareness:** Awareness of international aspects of CI/KR protection issues helps ensure implementation of effective, coordinated, and integrated CI/KR protection measures and helps enable CI/KR security partners to make informed decisions. Often these issues are not apparent to those who

can take the most effective action because of the complexity of the international systems affecting CI/KR protection. Awareness programs designed to identify such issues and provide the common framework that allows these issues to be effectively addressed by security partners are required for continued support for protection programs over the long term.

- **Education and Training:** NIPP training topics for managers and staff responsible for CI/KR that require emphasis include international considerations for CI/KR protection, because of the complex considerations that often accompany international linkages and initiatives. Because training and education programs can result in a higher quality workforce for international security partners, they provide benefits over entire careers rather than on a one-time basis as direct aid to international partners often does. Additionally, DHS will ensure that the organizational and sector expertise needed to implement the international aspects of the NIPP program over the long term is developed and maintained through exercises that include adequate testing of international CI/KR protection measures and plans.
- **Research and Development:** Cooperative and coordinated research efforts are one of the most effective ways to improve protective capabilities or to dramatically lower the costs of existing capabilities so that international security partners can afford to do more with their limited budgets. Techniques and designs developed through research can cost very little to share with international security partners, and although the lead-times needed for maturation of technology from the lab to the field can be decades, such improvements can have wider applicability or much greater effectiveness than available through with current methods.
- **Plan Update:** NIPP and SSP update proceeds according to a specified schedule; however, the international situation often changes in unpredictable ways and NIPP and SSP updates must be coordinated as required with international agreements affecting CI/KR protection.

H.7 Key Implementation Actions

Key actions needed to meet the goals for the international aspects of CI/KR protection are centered on efforts that can enable protective measures in multiple sectors; these are integrated in the appropriate chapters throughout the NIPP and summarized in this section to provide an overall perspective.

These actions fall in three categories:

- Improving the effectiveness of international cooperation;
- Implementing existing agreements that affect CI/KR; and
- Addressing cross-sector and global issues.

All milestones are specified with respect to the date of final signature of the NIPP. If agencies are not able to meet milestones, they should notify the Secretary of Homeland Security in a letter specifying the reason and the date by which they will be able to achieve the milestone.

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
DHS	Create a secretariat function within DHS to monitor the CI/KR aspects of the Canada and Mexico Border Agreements and other international accords.	X						
DHS DOS	Review the charter and coordinating mechanisms of the interagency working group on international CI/KR protection outreach activities to ensure that it supports the NIPP.	X						

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
DHS SSAs SPs	Broaden awareness of international CI/KR protection issues of a global nature by: • Collecting examples of solutions to similar global problems (e.g., telecommunications, air control, cybersecurity); • Exploring the creation of a global culture of security for CI/KR with other countries, in regional forums, and within international organizations; and • Promoting exchange of information on these issues through joint exercises, expert forums, workshops, and training sessions.	X						
DHS DOS SPs	Define a comprehensive international CI/KR protection strategy for pursuing and: • Improving the effectiveness of international cooperation; • Implementing existing and developing new agreements that affect CI/KR; and • Addressing cross-sector and global issues.				X			
DHS SSAs SPs	Initiate risk assessments of high-priority cross-border CI/KR assets.				X			
DHS SSAs SPs	Define and begin implementation of protective measures for cross-border assets and assets with cross-border implications.				X			
DHS SSAs	Ensure that specific actions relevant to the Border Agreements are integrated into their planning efforts: • Review individual Sector-Specific Plans to ensure inclusion of the following: o CI/KR protection planning with Canada and Mexico; and o Identification of CI/KR assets with Canada and Mexico	X						
DHS DOS OFA	Review and consolidate for further action all U.S. international commitments that relate to CI/KR protection including bilateral agreements with Canada, Mexico and other countries, and multilateral agreements and commitments with NATO, the G8, the European Union, and the United Nations.						X	
DHS DOS	Develop and improve cooperation with foreign countries and international organizations that will materially improve U.S. CI/KR protection through programs that can enhance CI/KR protection in multiple sectors including identifying:	X						

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
	• CI/KR strengths in other countries; • International R&D opportunities; and • Key international partners who can help DHS enhance the Nation's CI/KR security.							
DHS DOS SSAs SPs	Identify U.S. CI/KR products that can be shared with international partners, such as protection methodologies, decision tools, best practices, lessons learned, protocols, procedures, and other pertinent information.		X					
DHS SSAs OFA SPs	DHS will work with SSAs, other Federal agencies, and international partners to develop protocols to protect key supply chains for CI/KR components.				X			
DHS SPs	Actions needed to enhance international cooperation on cybersecurity and telecommunications standards include the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge.							X
DHS SSAs SPs	Identify and define global CI/KR assets.	X						
DHS DOS SPs	Work with international partners to develop and begin implementation of models and metrics to assess CI/KR protection issues of a global nature.				X			
DHS SSAs SPs	Develop a comprehensive communication system to share critical information, intelligence, and laboratory diagnostics with select partners, and develop protocols to stockpile or quickly replace key CI/KR components of foreign manufacture.						X	
DHS DOS SSAs SPs	Develop and promote a multilateral strategy of cooperation addressing roles and responsibilities regarding protection for CI/KR of a global nature; Initiate development of joint protection measures for global CI/KR; and Initiate and promote actions to protect against, mitigate the effects of, respond to, and recover from disruptions to CI/KR of a global nature.						X	
DHS DOS SSAs SPs	Begin to identify foreign manufacturers of key U.S. CI/KR components; Develop protocols for sharing protection-related information with partners who have responsibility for CI/KR of a global nature; and Develop protocols to transmit alert information to partners regarding specific CI/KR threats.			X				
DHS	Develop and define the metrics that measure the effectiveness of the comprehensive international CI/KR protection strategy and institute the data collection						X	

Resp. Entity	Activity	30 Days	60 Days	90 Days	180 Days	270 Days	365 Days	Ongoing
	system that provides the information necessary to compute these metrics.							
KEY: SP = Security Partners, DHS = Department of Homeland Security, DOS = Department of State, SSAs = Sector-Specific Agencies, HSC = Homeland Security Council, OFA = Other Federal Agencies.								

1

2